Memorandum from the Office of the Inspector General

November 15, 2021

Jeremy P. Fisher

FINAL REPORT – AUDIT 2021-17247 – FEDERAL INFORMATION SECURITY MODERNIZATION ACT

Attached is the subject final report for your review and information. No response to this report is necessary.

If you have any questions, please contact Melissa L. Conforti, Senior Auditor, at (865) 633-7383 or Sarah E. Huffman, Director, Information Technology Audits, at (865) 633-7345. We appreciate the courtesy and cooperation received from your staff during the audit.

David P. Wheeler
Assistant Inspector General
(Audits and Evaluations)

MLC:KDS
Attachment
cc (Attachment):
TVA Board of Directors
Brett A. Atkins
Brandy A. Barbee
Andrea S. Brackett
Tammy C. Bramlett
Kenneth C. Carnes II
Melissa R. Crane
Buddy Eller
David B. Fountain
Gregory G. Jackson
Benjamin A. Jones
Melissa A. Livesey
Jeffrey J. Lyash
Jill M. Matthews
Todd E. McCarter
Joshua R. Thomas
John M. Thomas III
OIG File No. 2021-17247

Office of the Inspector General

Audit Report

To the Vice President and Chief Information and Digital Officer, Technology and Innovation

FEDERAL INFORMATION SECURITY MODERNIZATION ACT

Audit Team
Melissa L. Conforti
Jonathan B. Anderson

Audit 2021-17247
November 15, 2021

ABBREVIATIONS

ATO	Authorization to Operate
DHS	Department of Homeland Security
FISMA	Federal Information Security Modernization Act of 2014
FY	Fiscal Year
IG	Inspector General
ISCM	Information Security Continuous Monitoring
ISP	Information Security Program
SCRM	Supply Chain Risk Management
TVA	Tennessee Valley Authority

TABLE OF CONTENTS

APPENDICES

Audit 2021-17247 – Federal Information Security Modernization Act

EXECUTIVE SUMMARY

Why the OIG Did This Audit

The Federal Information Security Modernization Act of 2014 (FISMA) requires each agency's Inspector General (IG) to conduct an annual independent evaluation to determine the effectiveness of the information security program (ISP) and practices of its respective agency.

Our objective was to determine the effectiveness of the Tennessee Valley Authority's (TVA) ISP and practices as defined by the *Fiscal Year* (FY) *2021 IG FISMA Reporting Metrics Version 1.1*. Our audit scope was limited to answering the IG FISMA metrics (defined in Appendix B).

What the OIG Found

During the course of this audit, we utilized the methodology and metrics in the IG FISMA metrics (as detailed in Appendix B) in our annual independent evaluation to determine the effectiveness of TVA's ISP. Each metric was assessed to determine its maturity level, as described in the following table.

FY 2021 IG FISMA Maturity Definitions	
Maturity Level	**Maturity Level Description**
Level 1: *Ad hoc*	Policies, procedures, and strategies are not formalized; activities are performed in an ad hoc, reactive manner.
Level 2: *Defined*	Policies, procedures, and strategies are formalized and documented, but not consistently implemented.
Level 3: *Consistently Implemented*	Policies, procedures, and strategies are consistently implemented, but quantitative and qualitative effectiveness measures are lacking.
Level 4: *Managed and Measurable*	Quantitative and qualitative measures on the effectiveness of policies, procedures, and strategies are collected across the organization and used to assess them and make necessary changes.
Level 5: *Optimized*	Policies, procedures, and strategies are fully institutionalized, repeatable, self-generating, consistently implemented, and regularly updated based on a changing threat and technology landscape and business/mission needs.

The IG FISMA metrics were organized into nine domains, which aligned with the following five function areas in the National Institute of Standards and Technology Framework for Improving Critical Infrastructure Cybersecurity: Identify, Protect, Detect, Respond, and Recover. Our analysis of the metric results was used to determine the overall function maturity levels presented on the following page.

Audit 2021-17247 – Federal Information Security Modernization Act

EXECUTIVE SUMMARY

FY 2021 IG FISMA Function Results		
Function	**Assessed Maturity Level**	**Rating**
Identify	4 – Managed and Measurable	Effective
Protect	4 – Managed and Measurable	Effective
Detect	4 – Managed and Measurable	Effective
Respond	4 – Managed and Measurable	Effective
Recover	4 – Managed and Measurable	Effective

Based on our analysis of the metrics and associated maturity levels defined within the IG FISMA metrics, we found TVA's ISP was operating in an effective manner.

BACKGROUND

The Federal Information Security Modernization Act of 2014 (FISMA) requires each agency's Inspector General (IG) to conduct an annual independent evaluation to determine the effectiveness of the information security program (ISP) and practices of its respective agency. The *Fiscal Year* (FY) *2021 IG FISMA Reporting Metrics Version 1.1* (see Appendix B) were developed by the Office of Management and Budget, the Department of Homeland Security (DHS), and the Council of the Inspectors General on Integrity and Efficiency, in consultation with the Federal Chief Information Officer Council and other stakeholders. The IG FISMA metrics were organized into nine domains, which aligned with the following five function areas in the National Institute of Standards and Technology Framework for Improving Critical Infrastructure Cybersecurity: Identify, Protect, Detect, Respond, and Recover. The FY 2021 IG FISMA functions and domains are shown in Table 1.

FY 2021 FISMA Functions and Corresponding Domains	
Function	**Domain**
Identify	Risk Management Supply Chain Risk Management
Protect	Configuration Management Identity and Access Management Data Protection and Privacy Security Training
Detect	Information Security Continuous Monitoring (ISCM)
Respond	Incident Response
Recover	Contingency Planning

Table 1

At the time of our review, TVA had two remaining open recommendations from the FY 2020 FISMA audit report.[1] They included (1) ensuring contingency planning roles and responsibilities are filled in accordance with TVA policy and (2) updating the policy to define a process for assigning risk designations for all positions. Although these recommendations remained open at the time of this report, they did not impact TVA's function or domain maturity ratings because a simple majority was used to determine the results as defined in Appendix B.

The results of our review were provided to the Office of Management and Budget and DHS through the use of their online reporting tool on October 21, 2021.

[1] Audit Report 2020-15709, *Federal Information Security Modernization Act*, December 21, 2020.

OBJECTIVE, SCOPE, AND METHODOLOGY

Our objective was to determine the effectiveness of the Tennessee Valley Authority's (TVA) ISP and practices as defined by the *FY 2021 IG FISMA Reporting Metrics Version 1.1*. Our audit scope was limited to answering the IG FISMA metrics (defined in Appendix B). A complete discussion of our audit objective, scope, and methodology is included in Appendix A.

FINDINGS

The IG FISMA metrics consider cybersecurity functions at a level 4 (managed and measurable) to be at an effective level of security. Based on our analysis of the metrics and associated maturity levels defined within the IG FISMA metrics, we found TVA's ISP was operating in an effective manner. See Table 2 for individual function ratings.

FY 2021 IG FISMA Function Results

Function	Assessed Maturity Level	Rating
Identify	4 – Managed and Measurable	Effective
Protect	4 – Managed and Measurable	Effective
Detect	4 – Managed and Measurable	Effective
Respond	4 – Managed and Measurable	Effective
Recover	4 – Managed and Measurable	Effective

Table 2

IDENTIFY

The Identify function includes understanding the business context, the resources that support critical functions, and the related cybersecurity and supply chain risks. This understanding enables an organization to focus and prioritize efforts consistent with its risk management strategy and business needs. Within the context of the IG FISMA metrics, the Identify function includes the risk management and supply chain risk management (SCRM) domains.

The SCRM domain was an addition to the IG FISMA metrics in FY 2021. However, in order to provide agencies with sufficient time to fully implement the domain, the SCRM maturity level results were not to be considered in the final scoring of the Identify function. Therefore, we evaluated both domains separately, and then used the result of the risk management domain to determine the maturity level of the Identify function.

We found the risk management domain operating at level 4 (managed and measurable). Based on this result, we determined the Identify function was operating at a level 4 (managed and measurable) maturity level and effective. [2] See Table 3 on the following page for individual domain ratings.

[2] As described on page 2 of Appendix A, the maturity level of each function was determined using a simple majority rule of the most frequent resulting domain maturity level within that function.

FY 2021 IG FISMA IDENTIFY Results		
Domain	**Assessed Maturity Level**	**Rating**
Risk Management	4 – Managed and Measurable	Effective
SCRM	4 – Managed and Measurable	Effective

Table 3

The following provides a summary of the findings for both domains in the Identify function.

Risk Management
In summary, we found TVA has generally implemented appropriate policies and procedures to identify and monitor risks across TVA. TVA has integrated its (1) information security architecture with its systems development lifecycle, (2) governance structure to support the incorporation of roles and responsibilities for cybersecurity risk management and Enterprise Risk Management, and (3) enterprise-wide risk communication program to drive strategic and business decisions. Additionally, we found TVA has:

- Ensured the risk-based allocation of resources based on system categorization, including for the protection of high value assets.
- Performed and maintained an organization-wide cybersecurity and privacy risk assessment.
- Consistently implemented an enterprise-wide automated solution of cybersecurity risks.

SCRM
In summary, we found TVA has generally implemented appropriate strategy, policies, and procedures to incorporate supply chain risk, including supplier risk evaluations, into its enterprise-wide risk management program and continuous monitoring practices. TVA utilized qualitative and quantitative performance measures to assess the effectiveness of its SCRM program. Additionally, we found TVA has:

- Utilized lessons learned to improve its SCRM strategy.
- Provided on the job training for component authenticity and anti-counterfeit to designated personnel.

PROTECT

The Protect function supports the ability to limit or contain the impact of a potential cybersecurity event by developing and implementing appropriate safeguards to ensure delivery of critical infrastructure services. Within the context of the IG FISMA metrics, the Protect function includes the following four domains:

- Configuration Management

- Identity and Access Management
- Data Protection and Privacy
- Security Training

We evaluated each domain separately and then used the individual results to determine the overall maturity level of the Protect function. We found all four domains operating at level 4 (managed and measurable) maturity level. Based on these results, we determined the Protect function was operating at a level 4 (managed and measurable) maturity level and effective. See Table 4 for individual domain ratings.

FY 2021 IG FISMA PROTECT Results		
Domain	**Assessed Maturity Level**	**Rating**
Configuration Management	4 – Managed and Measurable	Effective
Identity and Access Management	4 – Managed and Measurable	Effective
Data Protection and Privacy	4 – Managed and Measurable	Effective
Security Training	4 – Managed and Measurable	Effective

Table 4

The following provides a summary of the findings for each of the four domains in the Protect function.

Configuration Management
In summary, we found TVA has generally implemented appropriate policies and procedures to address security configuration and change management across TVA. TVA utilized qualitative and quantitative performance measures to assess the effectiveness of flaw remediation processes and change control activities. Additionally, we found TVA has:

- Allocated resources in a risk-based manner.
- Employed automation to help maintain security configurations.

Identity and Access Management
In summary, we found TVA has generally developed and consistently implemented a comprehensive Identity, Credential, and Access Management (ICAM) policy, integrated its ICAM strategy with its enterprise architecture, and utilized automated mechanisms to manage its policies. Additionally, we found TVA has:

- Allocated roles and responsibilities in a risk based manner.
- Ensured access agreements, acceptable use agreements, and rules of behavior were maintained through automated processes.
- Securely managed remote configurations and connections.

Data Protection and Privacy

In summary, we found TVA has generally defined and implemented its privacy program, conducts independent reviews of its privacy program and utilized metrics that measure the effectiveness of its program. Additionally, we found TVA has:

- Obtained feedback on the content of its privacy awareness training.
- Conducted phishing exercises.
- Made updates to its privacy program.

Security Training

In summary, we found TVA has generally defined and consistently implemented its organizational security awareness strategy and utilized qualitative and quantitative performance measures to gauge the effectiveness of its security awareness and training strategies and plans. Additionally, we found TVA has allocated resources in a risk-based manner and held stakeholders accountable.

DETECT

The Detect function enables timely discovery of cybersecurity events by developing and implementing actions to identify their occurrence. Within the context of the IG FISMA metrics, the Detect function includes the ISCM domain. We evaluated the ISCM domain and determined it was operating at a level 4 (managed and measurable) maturity level. Based on this result, we determined the Detect function was operating at a level 4 (managed and measurable) maturity level and effective.

In summary, we found TVA has consistently implemented ISCM strategy, policies, and procedures, including supporting tools, to provide an organization-wide approach to ISCM. TVA utilized performance measures to assess the effectiveness of its ISCM program. Additionally, we found TVA has:

- Allocated resources in a risk-based manner and held stakeholders accountable.
- Integrated metrics on the effectiveness of its ISCM program across TVA.

RESPOND

The Respond function supports the ability to contain the impact of a potential cybersecurity event by developing and implementing actions to take when a cybersecurity event is detected. Within the context of the IG FISMA metrics, the Respond function includes the incident response domain. We evaluated the incident response domain and determined it was operating at a level 4 (managed and measurable) maturity level. Based on this result, we determined the Respond function was operating at a level 4 (managed and measureable) maturity level and effective.

In summary, we found TVA has consistently implemented its policies and procedures for the incident response program. TVA has utilized qualitative and quantitative performance metrics to assess its incident response program. Additionally, we found TVA has:

- Participated in the DHS EINSTEIN 3 Accelerated[3] program to monitor, detect, and proactively block cyberattacks or potential compromises.
- Consistently implemented accountable incident response roles and responsibilities.
- Received, retained, and utilized cyber threat indicators.

RECOVER

The Recover function supports timely recovery to normal operations to reduce the impact from a cybersecurity event. Activities within the Recover function develop and implement plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity event. Within the context of the IG FISMA metrics, the Recover function includes the contingency planning domain. We evaluated the contingency planning domain and determined it was operating at a level 4 (managed and measurable) maturity level. Based on this result, we determined the Recover function was operating at a level 4 (managed and measurable) maturity level and effective.

In summary, we found TVA has generally defined and communicated roles and responsibilities of stakeholders, designated appropriate teams to implement its contingency planning strategies, and defined procedures for contingency planning training. TVA has utilized qualitative and quantitative performance metrics to assess the effectiveness of its information system contingency plans. Additionally, we found TVA has:

- Ensured the results of Business Impact Assessments are (1) integrated with the enterprise risk management process and (2) used in conjunction with the risk register.
- Employed automated mechanisms to test system contingency plans and coordinated plans with external stakeholders appropriately.

CONCLUSION

Based on our analysis of the metrics and associated maturity levels defined with the IG FISMA metrics, we found TVA's ISP was operating in an effective manner.

[3] EINSTEIN 3 Accelerated is a federal government program that provides additional cybersecurity monitoring to participating agencies.

OBJECTIVE, SCOPE, AND METHODOLOGY

Our objective was to determine the effectiveness of the Tennessee Valley Authority's (TVA) information security program and practices as defined by the *Fiscal Year* (FY) *2021 Inspector General* (IG) *Federal Information Security Modernization Act of 2014* (FISMA) *Reporting Metrics Version 1.1* (see Appendix B). Our audit scope was limited to answering the IG FISMA metrics (defined in Appendix B). Our fieldwork was completed between June 2021 and October 2021.

To accomplish our objective, we:

- Inquired with personnel in the Technology and Innovation organization as necessary to gain an understanding and clarification of the policies, processes, and current state.
- Reviewed documentation provided by Technology and Innovation to corroborate our understanding and assess TVA's current state, including:
  - Relevant TVA agency-wide and business unit specific policies, procedures, and documents (such as Standard Programs and Processes and Work Instructions)
  - Information system inventories
  - Authorization to Operation (ATO)
  - ATO tracker
- Reviewed previous Office of Inspector General audit reports on TVA's (1) compliance with FISMA in 2020,[1] (2) Privacy Program,[2] and (3) Privileged Account Management[3] for relevant findings.
- Conducted a network access control walkthrough.
- Reviewed the two TVA business essential systems that had completed disaster recovery testing during FY 2021. Specifically for these two systems, we reviewed contingency plan test after action reports and information system contingency plans to validate (1) those identified with roles and responsibilities were involved in testing and (2) recommendations and lessons learned were communicated. In addition, we reviewed business impact analysis documentation for completeness and accuracy.
- Reviewed the six TVA ATO packages that were completed for initialization or reauthorization during FY 2021. Specifically for these six ATO packages, we reviewed the authorization letter, system security plan, and risk and vulnerability reports to validate system level risk assessments, control baselines, security controls, and assigned roles and responsibilities.

---

1 Audit Report 2020-15709, *Federal Information Security Modernization Act*, December 21, 2020.

2 Audit Report 2021-15779, *TVA's Privacy Program*, September 20, 2021.

3 Audit Report 2021-15777, *Privileged Account Management*, September 22, 2021.

During the course of this audit, we determined the overall effectiveness of TVA's information security program by assessing the IG FISMA metrics (as detailed in Appendix B) on a maturity model spectrum. Table 1 details the five maturity model levels.

FY 2021 IG FISMA Maturity Definitions	
Maturity Level	**Maturity Level Description**
Level 1: *Ad-hoc*	Policies, procedures, and strategies are not formalized; activities are performed in an ad-hoc, reactive manner.
Level 2: *Defined*	Policies, procedures, and strategies are formalized and documented, but not consistently implemented.
Level 3: *Consistently Implemented*	Policies, procedures, and strategies are consistently implemented, but quantitative and qualitative effectiveness measures are lacking.
Level 4: *Managed and Measurable*	Quantitative and qualitative measures on the effectiveness of policies, procedures, and strategies are collected across the organization and used to assess them and make necessary changes.
Level 5: *Optimized*	Policies, procedures, and strategies are fully institutionalized, repeatable, self-generating, consistently implemented, and regularly updated based on a changing threat and technology landscape and business/mission needs.

Table 1

The maturity level of each domain was determined by answering the related IG FISMA metrics and using a simple majority rule of the most frequent resulting maturity levels, using the higher level when two or more levels are the frequently most rated an equal number of times. The maturity level of each function was determined using a simple majority rule of the most frequent resulting domain maturity level within that function. Overall effectiveness was determined using a simple majority rule of the function effectiveness results.

We conducted this performance audit in accordance with generally accepted government auditing standards. Those standards require we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

FY 2021
Inspector General
Federal Information
Security Modernization Act of 2014
(FISMA) Reporting Metrics
Version 1.1

May 12, 2021

Document History

Version	Date	Comments	Sec/Page
1.0	02/19/2021	Initial draft	All
1.0	Various	Updated criteria references throughout the metrics	All
1.0	Various	Added a Frequently Asked Question (FAQ) Section	Pg. 10
1.0	Various	Incorporated the overall questions related to the extent of implementation of policies and procedures within individual metrics	Throughout domains
1.0	Various	Clarified metric questions related to the integration of cybersecurity risk management and enterprise risk management	Q's 5, 7, 9, and 10
1.0	Various	Added a new metric on vulnerability disclosure practices	Q 24
1.0	3/12/2021	Draft issued for comment	All
1.1	4/6/2021 – 5/12/2021	Addressed comments received	Various
1.1	5/12/2021	Included a proposed weighted average maturity calculation for consideration in a future update to these metrics	Pg. 10-11
1.1	5/12/2021	Added a new Supply Chain Risk Management domain within Identify, which will not affect the framework function score.	Pg. 23-26
1.1	5/12/2021	Final issued	All

Contents

GENERAL INSTRUCTIONS

Overview

The Federal Information Security Modernization Act of 2014 (FISMA) requires each agency Inspector General (IG), or an independent external auditor, to conduct an annual independent evaluation to determine the effectiveness of the information security program and practices of its respective agency. Accordingly, the fiscal year (FY) 2021 IG FISMA Reporting Metrics contained in this document provide reporting requirements across key areas to be addressed in the independent evaluations of agencies' information security programs.

Submission Deadline

In accordance with FISMA and Office of Management and Budget (OMB) Memorandum M-21-02, *Fiscal Year 2020-2021 Guidance on Federal Information Security and Privacy Management Requirements*, all Federal agencies are to submit their IG metrics into the Department of Homeland Security's (DHS) CyberScope application by October 29, 2021. IG evaluations should reflect the status of agency information security programs from the completion of testing/fieldwork conducted for FISMA in 2021. Furthermore, IGs are encouraged to work with management at their respective agencies to establish a cutoff date to facilitate timely and comprehensive evaluation of the effectiveness of information security programs and controls.

Background and Methodology

The FY 2021 IG FISMA Reporting Metrics were developed as a collaborative effort amongst OMB, DHS, and the Council of the Inspectors General on Integrity and Efficiency (CIGIE), in consultation with the Federal Chief Information Officer (CIO) Council and other stakeholders. The FY 2021 metrics represent a continuation of work begun in FY 2016, when the IG metrics were aligned with the five function areas in the *National Institute of Standards and Technology (NIST) Framework for Improving Critical Infrastructure Cybersecurity* (Cybersecurity Framework): Identify, Protect, Detect, Respond, and Recover. The Cybersecurity Framework provides agencies with a common structure for identifying and managing cybersecurity risks across the enterprise and provides IGs with guidance for assessing the maturity of controls to address those risks.

Table 1 below provides an overview of the IG metrics by NIST Cybersecurity Framework (CSF) function area and related categories. The FY 21 IG metrics include a new Supply Chain Risk Management domain within the Identify function area.

Table 1: IG Metrics and NIST Cybersecurity Framework Function Areas and Categories

IG Metric Function Area and Related Domains[1]	Related CSF Categories
Identify (Risk Management)	Asset Management (ID.AM), Business Environment (ID.BE), Governance (ID.GV), Risk Assessment (ID.RA), and Risk Management Strategy (ID.RM)
Identify (Supply Chain Risk Management)	Supply Chain Risk Management (ID.SC)
Protect (Configuration Management)	Information Protection Processes and Procedures (PR.IP)
Protect (Identity and Access Management)	Identity Management and Access Control (PR.AC)
Protect (Data Protection and Privacy)	Data Security (PR.DS)
Protect (Security Training)	Awareness and Training (PR.AT)
Detect (Information Security Continuous Monitoring)	Security Continuous Monitoring (DE.CM)
Respond (Incident Response)	Response Planning (RS.RP), Communications (RS.CO), Analysis (RS.AN), Mitigation (RS.MI), and Improvements (RS.IM)
Recover (Contingency Planning)	Recovery Planning (RC.RP), Improvements (RC.IM), and Communications (RC.CO)

IGs are required to assess the effectiveness of information security programs on a maturity model spectrum, in which the foundational levels ensure that agencies develop sound policies and procedures and the advanced levels capture the extent that agencies institutionalize those policies and procedures. Table 2 below details the five maturity model levels: ad hoc, defined, consistently implemented, managed and measurable, and optimized.[2] Within the context of the maturity model, a Level 4, *Managed and Measurable*, information security program is operating at an effective level of security. NIST provides additional guidance for determining effectiveness of security controls.[3] IGs should consider both their and management's assessment of the unique missions, resources, and challenges when assessing the maturity of information security programs. Management's consideration of agency mission, resources, and challenges should be documented in the agency's assessment of risk as discussed in OMB Circular A-123, the U.S. Government Accountability Office's (GAO) Green Book, and NIST SP 800-37/800-39.

[1] Please refer to the NIST glossary available at https://csrc.nist.gov/glossary for definitions of the function areas and domains.

[2] The maturity level descriptions outlined in Table 2 provide foundational principles that guided the definition of the specific maturity level indicators and capabilities outlined in the IG metric questions. IGs should consider these descriptions when concluding on the overall effectiveness of specific functions, domains, and the information security program overall.

[3] *NIST Special Publication (SP) 800-53, Rev. 5, Security and Privacy Controls for Information Systems and Organizations*, defines security control effectiveness as the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the information system in its operational environment or enforcing/mediating established security policies.

Table 2: IG Evaluation Maturity Levels

Maturity Level	Maturity Level Description
Level 1: Ad-hoc	Policies, procedures, and strategies are not formalized; activities are performed in an ad-hoc, reactive manner.
Level 2: Defined	Policies, procedures, and strategies are formalized and documented but not consistently implemented.
Level 3: Consistently Implemented	Policies, procedures, and strategies are consistently implemented, but quantitative and qualitative effectiveness measures are lacking.
Level 4: Managed and Measurable	Quantitative and qualitative measures on the effectiveness of policies, procedures, and strategies are collected across the organization and used to assess them and make necessary changes.
Level 5: Optimized	Policies, procedures, and strategies are fully institutionalized, repeatable, self-generating, consistently implemented, and regularly updated based on a changing threat and technology landscape and business/mission needs.

FISMA Metrics Ratings

As noted earlier, each agency has a unique mission, cybersecurity challenges, and resources to address those challenges. Within the maturity model context, agencies should perform a risk assessment and identify the optimal maturity level that achieves cost-effective security based on their missions and risks faced, risk appetite, and risk tolerance level. The results of this assessment should be considered by IGs when determining effectiveness ratings with respect to the FISMA metrics. For example, if an agency has defined and formalized specific parameters (e.g. control parameters/tailoring decisions documented in security plans/risk assessments), IGs should consider the applicability of these parameters and determine whether to consider these when making maturity determinations.

Ratings throughout the nine domains will be determined by a simple majority, where the most frequent level (i.e. mode) across the questions will serve as the domain rating. For example, if there are seven questions in a domain, and the agency receives Defined ratings for three questions and Managed and Measurable ratings for four questions, then the domain rating is Managed and Measurable. OMB and DHS will ensure that these domain ratings are automatically scored when entered into CyberScope, and IGs and CIOs should note that these scores will rate the agency at the higher level in instances when two or more levels are the most frequently rated.

Similar to FY 2020, IGs have the discretion to determine the overall effectiveness rating and the rating for each of the Cybersecurity Framework functions (e.g., Protect, Detect) at the maturity level of their choosing. For FY 2021, IG's also have the discretion to determine the overall effectiveness rating at the domain (e.g., supply chain risk management, configuration management) level. Using this approach, the IG may determine that a particular domain, function area, and/or the agency's information security program is effective at maturity level lower than Level 4. The rationale for this is to provide greater flexibility for the IGs, while considering the agency-specific factors discussed above.

OMB strongly encourages IGs to use the domain ratings to inform the overall function ratings, and to use the five function ratings to inform the overall agency rating. For example, if the majority of an agency's ratings in the Protect-Configuration Management, Protect-Identity and Access Management, Protect-Data

Protection and Privacy, and Protect-Security Training domains are Managed and Measurable, the IGs are encouraged to rate the agency's Protect function as Managed and Measurable. Similarly, IGs are encouraged to apply the same simple majority rule described above to inform the overall agency rating. IGs should provide comments in CyberScope to explain the rationale for their effectiveness ratings. Furthermore, in CyberScope, IGs will be required to provide comments explaining the rationale for why a given metric is rated lower than a Level 4 maturity. Comments in CyberScope should reference how the agency's risk appetite and tolerance level with respect to cost-effective security, including compensating controls, were factored into the IGs decision.

Key Changes to the FY 2021 IG FISMA Metrics

One of the goals of the annual FISMA evaluations is to assess agencies' progress toward achieving outcomes that strengthen Federal cybersecurity, including implementing the Administration's priorities and best practices. One such area is increasing the maturity of the Federal government's Supply Chain Risk Management (SCRM) practices. As noted in the Federal Acquisition Supply Chain Security Act of 2018, agencies are required to assess, avoid, mitigate, accept, or transfer supply chain risks. The FY 2021 IG FISMA Reporting Metrics include a new domain on Supply Chain Risk Management (SCRM) within the Identify function. This new domain focuses on the maturity of agency SCRM strategies, policies and procedures, plans, and processes to ensure that products, system components, systems, and services of external providers are consistent with the organization's cybersecurity and supply chain risk management requirements. The new domain references SCRM criteria in *NIST Special Publication (SP) 800-53, Rev. 5, Security and Privacy Controls for Information Systems and Organizations*. To provide agencies with sufficient time to fully implement NIST 800-53, Rev 5., in accordance with OMB A-130, these new metrics should not be considered for the purposes of the Identify framework function rating.

Also, within the Identify function, specific metric questions have been reorganized and reworded to focus on the degree to which cyber risk management processes are integrated with enterprise risk management (ERM) processes. As an example, IGs are directed to evaluate how cybersecurity risk registers are used to communicate information at the information system, mission/business process, and organizational levels. These changes are consistent with NIST Interagency Report 8286, "Integrating Cybersecurity and Enterprise Risk Management (ERM)," which provides guidance to help organizations improve the cybersecurity risk information they provide as inputs to their enterprise ERM programs.[4]

Furthermore, OMB has issued guidance on improving vulnerability identification, management, and remediation. Specifically, Memorandum M-20-32, Improving Vulnerability Identification, Management, and Remediation, September 2, 2020, provides guidance to federal agencies on collaborating with members of the public to find and report vulnerabilities on federal information systems. In addition, DHS Binding Operational Directive 20-01, Develop and Publish a Vulnerability Disclosure Policy, September 2, 2020, provides guidance on the development and publishing of an agency's vulnerability disclosure policy and supporting handling procedures. The IG FISMA Reporting Metrics include a new question (#24) to measure the extent to which agencies utilize a vulnerability disclosure policy (VDP) as part of their vulnerability management program for internet-accessible federal systems.

In addition, the IG metric questions related to the implementation of policies and procedures have been reorganized and streamlined to reduce duplication and redundancies. Furthermore, a new Frequently Asked Question's (FAQ) section provides additional guidance to IGs.

[4] NISTIR 8286, *Integrating Cybersecurity and Enterprise Risk Management (ERM)*, October 2020.

FISMA Metrics Evaluation Guide

One of the goals of the maturity model reporting approach is to ensure consistency in IG FISMA evaluations across the Federal government. To that end in FY 2018, a collaborative effort amongst OMB, DHS, and CIGIE was undertaken to develop an evaluation guide to accompany the IG FISMA metrics. The guide is designed to provide a baseline of suggested sources of evidence that can be used by IGs as part of their FISMA evaluations. The guide also includes suggested types of analysis that IGs may perform to assess capabilities in given areas. In FY 2019, the evaluation guide was strengthened to include more detailed testing steps and methodologies for IGs to utilize in the function area of Identify (Risk Management). While updates to the evaluation guide were not made in FY 2020, OMB, DHS, and CIGIE plan to continue to enhance the evaluation guide to cover all function areas.[5]

[5] Updates to the evaluation guide will be posted on the DHS FISMA website subsequent to issuance of the metrics.

Frequently Asked Questions

1. To what extent should IGs utilize NIST SP 800-53, Rev. 5, as criteria for FISMA FY 2021 evaluations?

   - In accordance with OMB A-130, agencies are expected to meet the requirements of, and be in compliance with, NIST standards and guidelines within one year of their respective publication dates unless otherwise directed by OMB. The one-year compliance date for revisions to NIST publications applies only to new or updated material in the publications. For information systems under development or for legacy systems undergoing significant changes, agencies are expected to meet the requirements of, and be in compliance with, NIST standards and guidelines immediately upon deployment of the systems.

   - The IG FISMA metrics reference NIST SP 800-53, Rev. 4 criteria for all domains, except the SCRM domain. As applicable and in accordance with OMB A-130, IGs should utilize NIST SP 800-53, Rev. 5 as criteria for systems under development or legacy systems undergoing significant changes. Due to government-wide priorities and focus areas, IGs should utilize NIST 800-53, Rev. 5 as criteria for determining agency maturity in the SCRM domain and related metrics.

2. Do agencies need to meet all (100%) of the maturity indicators and criteria for previous levels before they can be rated at a higher maturity level?

   - No. FISMA requires agencies to provide information security protections commensurate with the risk and magnitude of the harm resulting from unauthorized access, use, disclosure, disruption, modification, or destruction of information and in information systems. As noted earlier, IGs should consider both their and management's assessment of the unique missions, resources, and challenges when assessing the maturity of information security programs. As such, IGs should use a risk-based approach when determining the impact of control deficiencies on overall maturity levels. IGs are encouraged not to use total compliance across maturity indicators and IG test cases, by itself, as a sole determinant of agency maturity.

3. Does a control exception (one or a few) identified in a sample automatically preclude an Agency from receiving a particular maturity rating?

   - No. As noted above, IGs should use a risk-based approach when determining the impact of control deficiencies on overall maturity levels. IGs are encouraged not to use total compliance across maturity indicators and IG test cases, by itself, as a sole determinant of agency maturity. IG should consider compensating controls and other agency-specific risk factors.

4. With respect to the Identity-Risk Management section, updates have been made to questions on cybersecurity and enterprise risk management. Are IGs being directed to audit or evaluate agencies' enterprise risk management programs?

   - No. The intent of these questions is to gauge the degree of integration between cyber risk management and ERM. IGs are encouraged to refer to NIST Interagency Report 8286, Integrating Cybersecurity and Enterprise Risk Management, for additional information.

Proposed Weighted Metrics Calculation

Since the FY 2017 FISMA reporting process, IGs have been directed to utilize a mode-based scoring approach to assess agency maturity levels. Under this approach, ratings throughout the reporting domains were determined by a simple majority, where the most frequent level (i.e., the mode) across the questions served as the domain rating. The same logic was applied at the function and overall information security program level. While this approach has provided an important baseline measure of the maturity of agencies' information security programs, all the metric questions have been weighted equally.

To drive continued improvements in cybersecurity maturity across the federal landscape and focus agency efforts, this document introduces a pilot concept of weighting specific FISMA metrics for assessment and scoring. Ten priority metrics, shown in Table 3, have been proposed based on a combination of the lowest average performing metrics from previous assessments, administration priorities, and the highest value controls. As part of the proposed weighted average approach to scoring, these priority metrics would be weighted twice as much in the maturity calculation, which is described in greater detail below. This pilot approach will help evaluate the impacts of these metrics and prepare agencies for the possibility of changing the calculation process in a future update to this document.

The overall maturity of the agency's information security program would be calculated based on the average rating of the individual function areas (Identify, Protect, Detect, Respond, and Recover). For example, if the weighted average maturity of two of the function areas is Level 3 – Consistently Implemented, and Level 4 – Managed and Measurable for the remaining three areas, then the information security program rating (average of 3.60) would be Level 4 – Managed and Measurable. The outcomes of this pilot will be shared with the CISO council and CIGIE for further consideration. Table 4 below provides a hypothetical example of an IG evaluation for the Identify-Risk Management area. Priority metrics within the Identity-Risk Management domain are highlighted in blue.

Table 3: Proposed Priority Metrics

Metric	Description	Cybersecurity Function and Domain	Reason
5	Cybersecurity risk management and integration with enterprise risk management (ERM)	Identify – Risk Management	Supports Administration's focus to improve integration of cybersecurity risk management within broader organizational risk management to help drive conversations for additional cybersecurity resources.
10	Automated view of risk	Identify – Risk Management	Improves government's ability to report and analyze cybersecurity data for use in decision making, supports Administration's focus on automated reporting.
31	Strong authentication measures – privileged users	Protect – Identity and Access Management	Supports Administration's focus on zero trust architectures, reducing privilege escalation, and implementation of M-19-17.
32	Least privilege and separation of duties	Protect – Identity and Access Management	Supports Administration's focus on zero trust architectures, reducing privilege escalation, and implementation of M-19-17.
36	PII security controls	Protect – Data Protection and Privacy	Supports Administration's focus on encrypting data at rest and in transit.
37	Security controls for exfiltration	Protect – Data Protection and Privacy	Supports Administration's focus on encrypting data at rest and in transit.
47	Information Security Continuous Monitoring (ISCM) policies and strategy	Detect – ISCM	Improves government's ability to report and analyze cybersecurity data for use in decision making, supports Administration's focus on automated reporting.
54	Incident detection and analysis	Respond – Incident Response	Supports Administration's focus on continued improvement of incident detection and handling to both address Congressional inquiries, as well as improving the government's ability to better identify and respond to the continued advancement of tactics used by adversaries around the world.
55	Incident handling	Respond – Incident Response	Supports Administration's focus on continued improvement of incident detection and handling to both address Congressional inquiries, as well as improving the government's ability to better identify and respond to the continued advancement of tactics used by adversaries around the world.
63	Testing of information system contingency plans	Recover – Contingency Planning	Critical component to Continuity of Operations Plans (COOPs), where rapid shift to telework from COVID-19 and SolarWinds incidents are recent examples of the importance of testing these plans.

Table 4: Example of Proposed Weighted Average Maturity Calculation

Metric Number	Metric Descriptor	IG Rating (Weight)	Weighted Factor
1	Inventory	Level 4 (1)	4
2	Hardware asset management	Level 3 (1)	3
3	Software asset management	Level 2 (1)	2
4	System categorization	Level 4 (1)	4
5	Cybersecurity risk management and integration with ERM	Level 2 (2)	4
6	Information security architecture	Level 4 (1)	4
7	Roles and responsibilities	Level 3 (1)	3
8	POA&M	Level 3 (1)	3
9	Risk communication	Level 4 (1)	4
10	Automated View of Risk	Level 3 (2)	6
Total		12*	37

* The *Weighted Average* is calculated by multiplying selected metrics by the Priority Metric Weight of 2.0 and then dividing the new total for each domain. For example, the Risk Management domain has 10 metrics of which 2 are Priority metrics so the total maturity for this domain is then divided by 12 instead of 10.)

Weighted Average Maturity = 3.08 = Level 3 Consistently Implemented[6]

This same approach would be used for all domains and function areas. The rating for the Protect function is a weighted average of all metrics in the domains that comprise the Protect function, such as the Protect-Configuration Management, Protect-Identity and Access, Protect-Security Training, and Protect-Data Protection and Privacy domains. The overall information security program maturity rating is then an average of the function level ratings.

[6] Weighted average maturities will be calculated to two decimal points and rounded to the nearest whole number (i.e., if the number after the decimal point is less than 5, it will be rounded down to the next lower maturity level; if the number is greater than or equal to 5, it will be rounded up to the next higher maturity level).

IDENTIFY FUNCTION AREA

Table 5: Risk Management

Question	Maturity Level				
	Ad Hoc	Defined	Consistently Implemented	Managed and Measurable	Optimized
1. To what extent does the organization maintain a comprehensive and accurate inventory of its information systems (including cloud systems, public facing websites, and third-party systems), and system interconnections (NIST SP 800-53. Rev. 4: CA-3, PM-5, and CM-8; NIST Cybersecurity Framework (CSF): ID.AM-1 – 4; FY 2021 CIO FISMA Metrics: 1.1, 1.1.5 and 1.4, OMB A-130, NIST SP 800-37, Rev. 2: Task P-18).	The organization has not defined its policies, procedures, and processes for developing and maintaining a comprehensive and accurate inventory of its information systems and system interconnections.	The organization has defined its policies, procedures, and processes for developing and maintaining a comprehensive and accurate inventory of its information systems and system interconnections.	The organization maintains a comprehensive and accurate inventory of its information systems (including cloud systems, public-facing websites, and third-party systems), and system interconnections.	The organization ensures that the information systems included in its inventory are subject to the monitoring processes defined within the organization's ISCM strategy.	The organization uses automation to develop and maintain a centralized information system inventory that includes hardware and software components from all organizational information systems. The centralized inventory is updated in a near-real time basis.

FY 2021 Inspector General FISMA Reporting Metrics v1.1
Identify Function Area (Risk Management)

Question	Maturity Level				
	Ad Hoc	Defined	Consistently Implemented	Managed and Measurable	Optimized
2. To what extent does the organization use standard data elements/taxonomy to develop and maintain an up-to-date inventory of hardware assets (including GFE and Bring Your Own Device (BYOD) mobile devices) connected to the organization's network with the detailed information necessary for tracking and reporting (NIST SP 800-53 Rev. 4: CA-7 and CM-8; NIST SP 800-137; NIST IR 8011; Federal Enterprise Architecture (FEA) Framework, v2; FY 2021 CIO FISMA Metrics: 1.2, 1.3, 2.2, 3.9, CSF: ID.AM-1; NIST SP 800-37, Rev. 2: Task P-10).	The organization has not defined policies, procedures, and processes for using standard data elements/taxonomy to develop and maintain an up-to-date inventory of hardware assets connected to the organization's network with the detailed information necessary for tracking and reporting.	The organization has defined policies, procedures, and processes for using standard data elements/taxonomy to develop and maintain an up-to-date inventory of hardware assets connected to the organization's network with the detailed information necessary for tracking and reporting.	The organization consistently utilizes its standard data elements/taxonomy to develop and maintain an up-to-date inventory of hardware assets connected to the organization's network and uses this taxonomy to inform which assets can/cannot be introduced into the network.	The organization ensures that the hardware assets connected to the network are covered by an organization-wide hardware asset management capability and are subject to the monitoring processes defined within the organization's ISCM strategy. For mobile devices, the agency enforces the capability to deny access to agency enterprise services when security and operating system updates have not been applied within a given period based on agency policy or guidance.	The organization employs automation to track the life cycle of the organization's hardware assets with processes that limit the manual/procedural methods for asset management. Further, hardware inventories are regularly updated as part of the organization's enterprise architecture current and future states.

FY 2021 Inspector General FISMA Reporting Metrics v1.1
Identify Function Area (Risk Management)

Question	Maturity Level				
	Ad Hoc	Defined	Consistently Implemented	Managed and Measurable	Optimized
3. To what extent does the organization use standard data elements/taxonomy to develop and maintain an up-to-date inventory of the software and associated licenses used within the organization with the detailed information necessary for tracking and reporting (NIST SP 800-53 Rev. 4: CA-7, CM-8, and CM-10; NIST SP 800-137; NIST IR 8011; FEA Framework, v2; FY 2021 CIO FISMA Metrics: 1.2.5, 1.3.3, 1.3.9, 1.3.10, 3.10; CSF: ID.AM-2; NIST SP 800-37, Rev. 2: Task P-10)?	The organization has not defined policies, procedures, and processes for using standard data elements/taxonomy to develop and maintain an up-to-date inventory of software assets and licenses, including for mobile applications, utilized in the organization's environment with the detailed information necessary for tracking and reporting.	The organization has defined policies, procedures, and processes for using standard data elements/taxonomy to develop and maintain an up-to-date inventory of software assets and licenses, including for mobile applications, utilized in the organization's environment with the detailed information necessary for tracking and reporting.	The organization consistently utilizes its standard data elements/taxonomy to develop and maintain an up-to-date inventory of software assets and licenses, including for mobile applications, utilized in the organization's environment and uses this taxonomy to inform which assets can/cannot be introduced into the network.	The organization ensures that the software assets, including mobile applications as appropriate, on the network (and their associated licenses), are covered by an organization-wide software asset management (or Mobile Device Management) capability and are subject to the monitoring processes defined within the organization's ISCM strategy. For mobile devices, the agency enforces the capability to prevent the execution of unauthorized software (e.g., blacklist, whitelist, or cryptographic containerization).	The organization employs automation to track the life cycle of the organization's software assets (and their associated licenses), including for mobile applications, with processes that limit the manual/procedural methods for asset management. Further, software inventories are regularly updated as part of the organization's enterprise architecture current and future states.

FY 2021 Inspector General FISMA Reporting Metrics v1.1
Identify Function Area (Risk Management)

Question	Maturity Level				
	Ad Hoc	**Defined**	**Consistently Implemented**	**Managed and Measurable**	**Optimized**
4. To what extent has the organization categorized and communicated the importance/priority of information systems in enabling its missions and business functions, including for high value assets (NIST SP 800-53 Rev. 4: RA-2, PM-7, and PM-11; NIST SP 800-60; NIST SP 800-37 (Rev. 2); CSF: ID.BE-3, ID.AM-5, and ID.SC-2; FIPS 199; FY 2021 CIO FISMA Metrics: 1.1; OMB M-19-03; NIST SP 800-37, Rev. 2: Task C-2, C-3, P-4, P-12, P-13, S-1 – S-3, NIST IR 8170)?	The organization has not defined policies, procedures, and processes for categorizing, reviewing, and communicating the importance/priority of information systems in enabling its missions and business functions, including for high value assets, as appropriate. In addition, the organization has not defined its policies, procedures, and processes for controls allocation, selection, and tailoring based on the importance/priority of its information systems.	The organization has defined policies, procedures, and processes for categorizing, reviewing, and communicating the importance/priority of information systems in enabling its missions and business functions, including for high value assets, as appropriate. In addition, the organization has defined policies, procedures, and processes for controls allocation, selection and tailoring based on the importance/priority of its information systems.	The organization consistently implements its policies, procedures, and processes for system categorization, review, and communication, including for high value assets, as appropriate. Security categorizations consider potential adverse impacts to organization operations, organizational assets, individuals, other organizations, and the Nation. System categorization levels are used to guide risk management decisions, such as the allocation, selection, and implementation of appropriate control baselines.	The organization ensures the risk-based allocation of resources based on system categorization, including for the protection of high value assets, as appropriate, through collaboration and data-driven prioritization.	The organization utilizes impact-level prioritization for additional granularity, and cybersecurity framework profiles, as appropriate, to support risk-based decision-making.

FY 2021 Inspector General FISMA Reporting Metrics v1.1
Identify Function Area (Risk Management)

Question	Maturity Level				
	Ad Hoc	**Defined**	**Consistently Implemented**	**Managed and Measurable**	**Optimized**
5. To what extent does the organization ensure that information system security risks are adequately managed at the organizational, mission/business process, and information system levels (NIST SP 800-39; NIST SP 800-53 Rev. 4: RA-3, PM-9; NIST IR 8286, CSF: ID RM-1 – ID.RM-3; OMB A-123; OMB M-16-17; OMB M-17-25; NIST SP 800-37 (Rev. 2): Tasks P-2, P-3, P-14, R-2, and R-3?	The organization has not defined and communicated the policies, procedures and processes it utilizes to manage the cybersecurity risks associated with operating and maintaining its information systems. At a minimum, the policies, procedures, and processes do not cover the following areas from a cybersecurity perspective: - Risk Framing - Risk assessment - Risk response - Risk monitoring	The organization has defined and communicated the policies, procedures and processes it utilizes to manage the cybersecurity risks associated with operating and maintaining its information systems. The policies, procedures, and processes cover cybersecurity risk management at the organizational, mission/business process, and information system levels and address the following components - Risk Framing - Risk assessment - Risk response - Risk monitoring	The organization consistently implements its policies, procedures, and processes to manage the cybersecurity risks associated with operating and maintaining its information systems. The organization ensures that decisions to manage cybersecurity risk at the information system level are informed and guided by risk decisions made at the organizational and mission/business levels. System risk assessments are performed [according to organizational defined time frames] and appropriate security controls to mitigate risks identified are implemented on a consistent basis. The organization utilizes the common vulnerability scoring system, or similar approach, to communicate the characteristics and severity of software vulnerabilities. Further, the organization utilizes a cybersecurity risk register to manage risks, as appropriate, and is consistently capturing and sharing lessons learned on the effectiveness of cybersecurity risk management processes and updating the program accordingly.	The organization utilizes the results of its system level risk assessments, along with other inputs, to perform and maintain an organization-wide cybersecurity and privacy risk assessment. The result of this assessment is documented in a cybersecurity risk register and serve as an input into the organization's enterprise risk management program. The organization consistently monitors the effectiveness of risk responses to ensure that risk tolerances are maintained at an appropriate level. The organization ensures that information in cybersecurity risk registers is obtained accurately, consistently, and in a reproducible format and is used to (i) quantify and aggregate security risks, (ii) normalize cybersecurity risk information across organizational units, and (iii) prioritize operational risk response	The cybersecurity risk management program is fully integrated at the organizational, mission/business process, and information system levels, as well as with the entity's enterprise risk management program. Further, the organization's cybersecurity risk management program is embedded into daily decision making across the organization and provides for continuous identification and monitoring to ensure that risk remains within organizationally-defined acceptable levels. The organization utilizes Cybersecurity Framework profiles to align cybersecurity outcomes with mission or business requirements, risk tolerance, and resources of the organization.

FY 2021 Inspector General FISMA Reporting Metrics v1.1
Identify Function Area (Risk Management)

Question	Maturity Level				
	Ad Hoc	Defined	Consistently Implemented	Managed and Measurable	Optimized
6. To what extent does the organization utilize an information security architecture to provide a disciplined and structured methodology for managing risk, including risk from the organization's supply chain (Federal Information Technology Acquisition Reform Act (FITARA), NIST SP 800-39; NIST SP 800-160; NIST SP 800-37 (Rev. 2) Task P-16; OMB M-19-03; OMB M-15-14, FEA Framework; NIST SP 800-53 Rev. 4: PL-8, SA-3, SA-8, SA-9, SA-12, and PM-9; NIST SP 800-163, Rev. 1 CSF: ID.SC-1 and PR.IP-2; SECURE Technology Act: s. 1326)?	The organization has not defined an information security architecture and its processes for ensuring that new/acquired hardware/software, including mobile apps, are consistent with its security architecture prior to introducing systems into its development environment.	The organization has defined an information security architecture and described how that architecture is integrated into and supports the organization's enterprise architecture. In addition, the organization has defined how it implements system security engineering principles and software assurance processes for mobile applications, within its system development life cycle (SDLC).	The organization has consistently implemented its security architecture across the enterprise, business process, and system levels. System security engineering principles are followed and include assessing the impacts to the organizations information security architecture prior to introducing information system changes into the organization's environment. In addition, the organization employs a software assurance process for mobile applications.	The organization's information security architecture is integrated with its systems development lifecycle and defines and directs implementation of security methods, mechanisms, and capabilities to both the Information and Communications Technology (ICT) supply chain and the organization's information systems.	The organization uses advanced technologies and techniques for managing supply chain risks. To the extent practicable, the organization can quickly adapt its information security and enterprise architectures to mitigate supply chain risks.

FY 2021 Inspector General FISMA Reporting Metrics v1.1
Identify Function Area (Risk Management)

Question	Maturity Level				
	Ad Hoc	Defined	Consistently Implemented	Managed and Measurable	Optimized
7. To what extent have the roles and responsibilities of internal and external stakeholders involved in cybersecurity risk management processes been defined, communicated, and implemented across the organization (NIST SP 800-39: Section 2.3.1, 2.3.2, and Appendix D; NIST SP 800-53 Rev. 4: RA-1; CSF: ID.AM-6, ID.RM-1, and ID.GV-2; NIST IR 8286, Section 3.1.1, OMB A-123; NIST SP 800-37 (Rev. 2) Section 2.8 and Task P-1; OMB M-19-03)?	Roles and responsibilities for cybersecurity risk management have not been defined and communicated across the organization. Further, the organization has not defined the relevant work roles for stages in the cybersecurity risk management process and which roles are responsible, accountable, consulted, or informed about various activities, as appropriate. In addition, the organization has not defined the relationships between cybersecurity risk management roles and those roles involved with enterprise risk management.	Roles and responsibilities of stakeholders involved in cybersecurity risk management processes have been defined and communicated across the organization. This includes the relevant work roles for stages in the cybersecurity risk management process and which roles are responsible, accountable, consulted, or informed about various activities, as appropriate. In addition, the organization has defined and clearly communicated the relationships between cybersecurity risk management roles and those roles involved with enterprise risk management.	Individuals are consistently performing the cybersecurity risk management roles and responsibilities that have been defined across the organization. This includes roles and responsibilities related to integration with enterprise risk management processes, as appropriate.	Resources (people, processes, and technology) are allocated in a risk-based manner for stakeholders to effectively implement cybersecurity risk management activities and integrate those activities with enterprise risk management processes, as appropriate. Further, stakeholders involved in cybersecurity risk management are held accountable for carrying out their roles and responsibilities effectively.	The organization utilizes an integrated governance structure, in accordance with A-123, and associated review processes (e.g., ERM councils or IT investment review boards) to support the integration of roles and responsibilities for cybersecurity risk management and ERM.

FY 2021 Inspector General FISMA Reporting Metrics v1.1
Identify Function Area (Risk Management)

Question	Maturity Level				
	Ad Hoc	Defined	Consistently Implemented	Managed and Measurable	Optimized
8. To what extent has the organization ensured that plans of action and milestones (POA&Ms) are utilized for effectively mitigating security weaknesses (NIST SP 800-53 Rev. 4: CA-5; NIST SP 800-37 (Rev. 2) Task A-6, R-3; OMB M-04-14, M-19-03, CSF v1.1, ID.RA-6)?	Policies and procedures for the effective use of POA&Ms to mitigate security weaknesses have not been defined and communicated.	Policies and procedures for the effective use of POA&Ms have been defined and communicated. These policies and procedures address, at a minimum, the centralized tracking of security weaknesses, prioritization of remediation efforts, maintenance, and independent validation of POA&M activities.	The organization consistently utilizes POA&Ms to effectively mitigate security weaknesses. The organization utilizes a prioritized and consistent approach to POA&Ms that considers: • Security categorizations • Specific control deficiencies and their criticality • Rationale for accepting certain deficiencies in controls • POA&M attributes, in accordance with OMB M-04-14 (e.g., severity and brief description of the weakness and estimated funding resources required to resolve the weakness)	The organization monitors and analyzes qualitative and quantitative performance measures on the effectiveness of its POA&M activities and uses that information to make appropriate adjustments, as needed, to ensure that its risk posture is maintained.	The organization employs automation to correlate security weaknesses amongst information systems and identify enterprise-wide trends and solutions in a near real-time basis. Furthermore, processes are in place to identify and manage emerging risks, in addition to known security weaknesses.

FY 2021 Inspector General FISMA Reporting Metrics v1.1
Identify Function Area (Risk Management)

Question	Maturity Level				
	Ad Hoc	Defined	Consistently Implemented	Managed and Measurable	Optimized
9. To what extent does the organization ensure that information about cybersecurity risks is communicated in a timely and effective manner to appropriate internal and external stakeholders (OMB A-123; OMB Circular A-11 and OMB M-19-03; CSF: Section 3.3; NIST SP 800-37 (Rev. 2) Task M-5; SECURE Technology Act: s. 1326, NIST IR 8170 and 8286)?	The organization has not defined how cybersecurity risk information is communicated in a timely and effective manner to appropriate internal and external stakeholders.	The organization has defined how cybersecurity risks are communicated in a timely and effective manner to appropriate internal and external stakeholders. This includes the organizations policies, procedures, and processes for utilizing cybersecurity risk registers, or other comparable mechanisms, to share and coordinate cybersecurity risk activities.	The organization consistently utilizes a cybersecurity risk register, or other comparable mechanism to ensure that information about risks are communicated in a timely and effective manner to appropriate internal and external stakeholders with a need-to-know. Furthermore, the organization actively shares information with partners to ensure that accurate, current information is being distributed and consumed.	The organization employs robust diagnostic and reporting frameworks, including dashboards that facilitate a portfolio view of cybersecurity risks across the organization. The dashboard presents qualitative and quantitative metrics that provide indicators of cybersecurity risk. Cybersecurity risks are integrated into enterprise level dashboards and reporting frameworks. To facilitate timely, consistent, and effective communication of cybersecurity risks, the organization ensures that data supporting the cybersecurity risk register, or other comparable mechanism, are obtained accurately, consistently, and in a reproducible format and is used to - Quantify and aggregate security risks - Normalize information across organizational units - Prioritize operational risk response activities	Using risk profiles and dynamic reporting mechanisms, cybersecurity risk information is incorporated into the organization's enterprise risk management program and utilized to provide a fully integrated, prioritized, enterprise-wide view of organizational risks to drive strategic and business decisions. Cyber risks are normalized and translated at the organizational level to support a fully integrated, prioritized, enterprise-wide view of organizational risks to drive strategic and business decisions.

FY 2021 Inspector General FISMA Reporting Metrics v1.1
Identify Function Area (Risk Management)

Question	Maturity Level				
	Ad Hoc	Defined	Consistently Implemented	Managed and Measurable	Optimized
10. To what extent does the organization utilize technology/ automation to provide a centralized, enterprise wide (portfolio) view of cybersecurity risk management activities across the organization, including risk control and remediation activities, dependencies, risk scores/levels, and management dashboards (NIST SP 800-39; OMB A-123 and NIST IR 8286)?	The organization has not identified and defined its requirements for an automated solution to provide a centralized, enterprise wide (portfolio) view of cybersecurity risks across the organization, including risk control and remediation activities, dependences, risk scores/levels, and management dashboards.	The organization has identified and defined its requirements for an automated solution that provides a centralized, enterprise wide view of cybersecurity risks across the organization, including risk control and remediation activities, dependencies, risk scores/levels, and management dashboards.	The organization consistently implements an automated solution across the enterprise that provides a centralized, enterprise wide view of cybersecurity risks, including risk control and remediation activities, dependencies, risk scores/levels, and management dashboards. All necessary sources of cybersecurity risk information are integrated into the solution.	The organization uses automation to perform scenario analysis and model potential responses, including modeling the potential impact of a threat exploiting a vulnerability and the resulting impact to organizational systems and data. In addition, the organization ensures that cybersecurity risk management information is integrated into ERM reporting tools, such as a governance, risk management, and compliance tool), as appropriate	The organization has institutionalized the use of advanced technologies for analysis of trends and performance against benchmarks to continuously improve its cybersecurity risk management program.
11. Provide any additional information on the effectiveness (positive or negative) of the organization's risk management program that was not noted in the questions above. Taking into consideration the overall maturity level generated from the questions above and based on all testing performed, is the risk management program effective?					

FY 2021 Inspector General FISMA Reporting Metrics v1.1
Identify Function Area (Supply Chain Risk Management)

Table 6: Supply Chain Risk Management (SCRM)

Note: This section not to be considered in the Identity framework function rating

Question	Maturity Level				
	Ad Hoc	Defined	Consistently Implemented	Managed and Measurable	Optimized
12. To what extent does the organization utilize an organization wide SCRM strategy to manage the supply chain risks associated with the development, acquisition, maintenance, and disposal of systems, system components, and system services? (The Federal Acquisition Supply Chain Security Act of 2018 (H.R. 7327, 41 USC Chap. 13 Sub chap. III and Chap. 47, P.L. 115-390) (Dec. 21, 2018), NIST SP 800-53, Rev. 5, PM-30, NIST IR 8276)?	The organization has not defined and communicated an organization wide SCRM strategy.	The organization has defined and communicated an organization wide SCRM strategy. The strategy addresses: - SCRM risk appetite and tolerance - SCRM strategies or controls - Processes for consistently evaluating and monitoring supply chain risk - Approaches for implementing and communicating the SCRM strategy - Associated roles and responsibilities	The organization consistently implements its SCRM strategy across the organization and utilizes the strategy to guide supply chain analyses, communication with internal and external partners and stakeholders, and in building consensus regarding the appropriate resources for SCRM. Further, the organization utilizes lessons learned in implementation to review and update its SCRM strategy in an organization defined timeframe.	The organization monitors and analyzes qualitative and quantitative performance measures on the effectiveness of its SCRM strategy and makes updates, as appropriate. The organization ensures that data supporting metrics are obtained accurately, consistently, and in a reproducible format.	The organization's SCRM strategy is fully integrated with its enterprise risk management strategy and program. On a near real-time basis, the organization actively adapts its SCRM strategy to respond to evolving and sophisticated threats.

FY 2021 Inspector General FISMA Reporting Metrics v1.1
Identify Function Area (Supply Chain Risk Management)

Question	Maturity Level				
	Ad Hoc	Defined	Consistently Implemented	Managed and Measurable	Optimized
13. To what extent does the organization utilize SCRM policies and procedures to manage SCRM activities at all organizational tiers (The Federal Acquisition Supply Chain Security Act of 2018, NIST 800-53, Rev. 5, SR-1, NIST CSF v1.1, ID.SC-1 and ID.SC-5, NIST IR 8276)?	The organization has not defined and communicated its SCRM policies, procedures, and processes.	The organization has defined and communicated its SCRM policies, procedures, and processes. As appropriate, the policies and procedures are guided by the organization wide SCRM strategy (metric #12). At a minimum, the following areas are addressed - Procedures to facilitate the implementation of the policy and the associated baseline supply chain risk management controls as well as baseline supply chain related controls in other families. - Purpose, scope, SCRM roles and responsibilities, management commitment, and coordination amongst organization entities.	The organization consistently implements its policies, procedures, and processes for managing supply chain risks for [organizationally-defined] products, systems, and services provided by third parties. Further, the organization utilizes lessons learned in implementation to review and update its SCRM policies, procedures, and processes in an organization defined timeframe.	The organization monitors, analyzes, and reports on the qualitative and quantitative performance measures used to gauge the effectiveness of its SCRM policies and procedures and ensures that data supporting the metrics is obtained accurately, consistently, and in a reproducible format. The organization has integrated SCRM processes across its enterprise, including personnel security and physical security programs, hardware, software, and firmware development processes, configuration management tools, techniques, and measures to maintain provenance (as appropriate); shipping and handling procedures; and programs, processes, or procedures associated with the production and distribution of supply chain elements.	In a near real-time basis, the organization can update its SCRM policies, procedures, and processes, as appropriate, to respond to evolving and sophisticated threats.

FY 2021 Inspector General FISMA Reporting Metrics v1.1
Identify Function Area (Supply Chain Risk Management)

Question	Maturity Level				
	Ad Hoc	Defined	Consistently Implemented	Managed and Measurable	Optimized
14. To what extent does the organization ensure that products, system components, systems, and services of external providers are consistent with the organization's cybersecurity and supply chain requirements. (The Federal Acquisition Supply Chain Security Act of 2018, NIST SP 800-53 REV. 5: SA-4, SR-3, SR-5, SR-6 (as appropriate); NIST SP 800-152; FedRAMP standard contract clauses; Cloud Computing Contract Best Practices; OMB M-19-03; OMB A-130; CSF: ID.SC-2 through 4, NIST IR 8276).	The organization has not defined and communicated policies, procedures, and processes to ensure that [organizationally defined products, system components, systems, and services] adhere to its cybersecurity and supply chain risk management requirements.	The organization has defined and communicated policies and procedures to ensure that [organizationally defined products, system components, systems, and services] adhere to its cybersecurity and supply chain risk management requirements. The following components, at a minimum, are defined - The identification and prioritization of externally provided systems, system components, and services as well how the organization maintains awareness of its upstream suppliers - Integration of acquisition processes, including the use of contractual agreements that stipulate appropriate cyber and SCRM measures for external providers. - Tools and techniques to utilize the acquisition process to protect the supply chain, including, risk-based processes for evaluating cyber supply chain risks associated with third party providers, as appropriate. - Contract tools or procurement methods to confirm contractors are meeting their contractual SCRM obligations.	The organization ensures that its policies, procedures, and processes are consistently implemented for assessing and reviewing the supply chain-related risks associated with suppliers or contractors and the system, system component. In addition, the organization obtains sufficient assurance, through audits, test results, or other forms of evaluation, that the security and supply chain controls of systems or services provided by contractors or other entities on behalf of the organization meet FISMA requirements, OMB policy, and applicable NIST guidance. Furthermore, the organization maintains visibility into its upstream suppliers and can consistently track changes in suppliers. ,	The organization uses qualitative and quantitative performance metrics (e.g., those defined within SLAs) to measure, report on, and monitor the information security and SCRM performance of organizationally defined products, systems, and services provided by external providers. In addition, the organization has incorporated supplier risk evaluations, based on criticality, into its continuous monitoring practices to maintain situational awareness into the supply chain risks.	The organization analyzes, in a near-real time basis, the impact of material changes to security and SCRM assurance requirements on its relationships with external providers and ensures that acquisition tools, methods, and processes are updated as soon as possible.

FY 2021 Inspector General FISMA Reporting Metrics v1.1
Identify Function Area (Supply Chain Risk Management)

Question	Maturity Level				
	Ad Hoc	**Defined**	**Consistently Implemented**	**Managed and Measurable**	
15. To what extent does the organization ensure that counterfeit components are detected and prevented from entering the organization's systems? (800-53 rev 5 SR-11, 11 (1), and 11(2)	The organization has not defined and communicated its component authenticity policies and procedures.	The organization has defined and communicated its component authenticity policies and procedures. At a minimum the following areas are addressed: - Procedures to detect and prevent counterfeit components from entering the system. - Procedures to maintain configuration control over organizationally defined system components that are awaiting repair and service or repaired components awaiting return to service. - Requirements and procedures for reporting counterfeit system components	The organization consistently implements its component authenticity policies and procedures. Further, the organization: -Provides component authenticity/anti-counterfeit training for designated personnel. -Maintains configuration control over organizationally defined system components that are awaiting repair and service or repaired components awaiting return to service.	The organization monitors, analyzes, and reports on the qualitative and quantitative performance measures used to gauge the effectiveness of its component authenticity policies and procedures and ensures that data supporting the metrics is obtained accurately, consistently, and in a reproducible format. In addition, the organization has incorporated component authenticity controls into its continuous monitoring practices.	In a near real-time basis, the organization can update its supply chain risk management policies and procedures, as appropriate, to respond to evolving and sophisticated threats.
16. Provide any additional information on the effectiveness (positive or negative) of the organization's supply chain risk management program that was not noted in the questions above. Taking into consideration the overall maturity level generated from the questions above and based on all testing performed, is the risk management program effective?					

PROTECT FUNCTION AREA

Table 7: Configuration Management

Question	Maturity Level				
	Ad Hoc	Defined	Consistently Implemented	Managed and Measurable	Optimized
17. To what extent have the roles and responsibilities of configuration management stakeholders been defined, communicated, and implemented across the agency, and appropriately resourced (NIST SP 800-53 REV. 4: CM-1; NIST SP 800-128: Section 2.4)?	Roles and responsibilities at the organizational and information system levels for stakeholders involved in information system configuration management have not been fully defined and communicated across the organization.	Roles and responsibilities at the organizational and information system levels for stakeholders involved in information system configuration management have been fully defined and communicated across the organization.	Individuals are performing the roles and responsibilities that have been defined across the organization.	Resources (people, processes, and technology) are allocated in a risk-based manner for stakeholders to effectively perform information system configuration management activities. Further, stakeholders are held accountable for carrying out their roles and responsibilities effectively.	
18. To what extent does the organization utilize an enterprise wide configuration management plan that includes, at a minimum, the following components: roles and responsibilities, including establishment of a Change Control Board (CCB) or related body; configuration management processes, including processes for: identifying and managing configuration items during the appropriate phase within an organization's SDLC; configuration monitoring; and applying configuration management requirements to contractor operated systems (NIST SP 800-128: Section 2.3.2; NIST SP 800-53 REV. 4: CM-9)?	The organization has not developed an organization wide configuration management plan with the necessary components.	The organization has developed an organization wide configuration management plan that includes the necessary components.	The organization has consistently implemented an organization wide configuration management plan and has integrated its plan with its risk management and continuous monitoring programs. Further, the organization utilizes lessons learned in implementation to make improvements to its plan.	The organization monitors, analyzes, and reports to stakeholders qualitative and quantitative performance measures on the effectiveness of its configuration management plan, uses this information to take corrective actions when necessary, and ensures that data supporting the metrics is obtained accurately, consistently, and in a reproducible format.	The organization utilizes automation to adapt its configuration management plan and related processes and activities to a changing cybersecurity landscape on a near real-time basis (as defined by the organization).

FY 2021 Inspector General FISMA Reporting Metrics v1.1
Protect Function Area (Configuration Management)

Question	Maturity Level				
	Ad Hoc	Defined	Consistently Implemented	Managed and Measurable	Optimized
19. To what extent does the organization utilize baseline configurations for its information systems and maintain inventories of related components at a level of granularity necessary for tracking and reporting (NIST SP 800-53 REV. 4: CM-2 and CM-8; FY 2021 CIO FISMA Metrics: 2.2, 3.9.2, and 3.10.1; CSF: DE.CM-7 and PR.IP-1)?	The organization has not established policies and procedures to ensure that baseline configurations for its information systems are developed, documented, and maintained under configuration control and that system components are inventoried at a level of granularity deemed necessary for tracking and reporting.	The organization has developed, documented, and disseminated its baseline configuration and component inventory policies and procedures.	The organization consistently records, implements, and maintains under configuration control, baseline configurations of its information systems and an inventory of related components in accordance with the organization's policies and procedures. Further, the organization utilizes lessons learned in implementation to make improvements to its baseline configuration policies and procedures.	The organization employs automated mechanisms (such as application whitelisting and network management tools) to detect unauthorized hardware, software, and firmware and unauthorized changes to hardware, software, and firmware.	The organization utilizes technology to implement a centralized baseline configuration and information system component inventory process that includes information from all organization systems (hardware and software) and is updated in a near real-time basis.
20. To what extent does the organization utilize configuration settings/common secure configurations for its information systems? (NIST SP 800-53 REV. 4: CM-6, CM-7, RA-5, and SI-2; NIST SP 800-70, Rev. 4, FY 2021 CIO FISMA Metrics: 2.1, 2.2, 4.3; SANS/CIS Top 20 Security Controls 3.7; CSF: ID.RA-1 and DE.CM-8)?	The organization has not established policies and procedures for ensuring that configuration settings/common secure configurations are defined, implemented, and monitored.	The organization has developed, documented, and disseminated its policies and procedures for configuration settings/common secure configurations. In addition, the organization has developed, documented, and disseminated common secure configurations (hardening guides) that are tailored to its environment. Further, the organization has established a deviation process.	The organization consistently implements, assesses, and maintains secure configuration settings for its information systems based on the principle of least functionality. Further, the organization consistently utilizes SCAP-validated software assessing (scanning) capabilities against all systems on the network (see inventory from questions #1 - #3) to assess and manage both code-based and configuration-based vulnerabilities. The organization utilizes lessons learned in implementation to make improvements to its secure configuration policies and procedures	The organization employs automation to help maintain an up-to-date, complete, accurate, and readily available view of the security configurations for all information system components connected to the organization's network and makes appropriate modifications in accordance with organization-defined timelines.	The organization deploys system configuration management tools that automatically enforce and redeploy configuration settings to systems at frequent intervals as defined by the organization, or on an event driven basis.

FY 2021 Inspector General FISMA Reporting Metrics v1.1
Protect Function Area (Configuration Management)

Question	Maturity Level				
	Ad Hoc	Defined	Consistently Implemented	Managed and Measurable	Optimized
21. To what extent does the organization utilize flaw remediation processes, including patch management, to manage software vulnerabilities (NIST SP 800-53 REV. 4: CM-3, RA-5, SI-2, and SI-3; NIST SP 800-40, Rev. 3; SANS/CIS Top 20, Control 4.5; FY 2021 CIO FISMA Metrics: 1.3.7, 1.3.8, 2.13, 2.14; CSF: ID.RA-1; DHS Binding Operational Directives (BOD) 18-02 and 19-02)?	The organization has not developed, documented, and disseminated its policies and procedures for flaw remediation, including for mobile devices (GFE and non-GFE).	The organization has developed, documented, and disseminated its policies and procedures for flaw remediation, including for mobile devices. Policies and procedures include processes for: identifying, reporting, and correcting information system flaws, testing software and firmware updates prior to implementation, installing security relevant updates and patches within organizational-defined timeframes, and incorporating flaw remediation into the organization's configuration management processes.	The organization consistently implements its flaw remediation policies, procedures, and processes and ensures that patches, hotfixes, service packs, and anti-virus/malware software updates are identified, prioritized, tested, and installed in a timely manner. In addition, the organization patches critical vulnerabilities within 30 days and utilizes lessons learned in implementation to make improvements to its flaw remediation policies and procedures.	The organization centrally manages its flaw remediation process and utilizes automated patch management and software update tools for operating systems, where such tools are available and safe. The organization monitors, analyzes, and reports qualitative and quantitative performance measures on the effectiveness of flaw remediation processes and ensures that data supporting the metrics is obtained accurately, consistently, and in a reproducible format.	The organization utilizes automated patch management and software update tools for all applications and network devices (including mobile devices), as appropriate, where such tools are available and safe. As part its flaw remediation processes, the organization performs deeper analysis of software code, such as through patch sourcing and testing

FY 2021 Inspector General FISMA Reporting Metrics v1.1
Protect Function Area (Configuration Management)

Question	Maturity Level				
	Ad Hoc	Defined	Consistently Implemented	Managed and Measurable	Optimized
22. To what extent has the organization adopted the Trusted Internet Connection (TIC) program to assist in protecting its network (OMB M-19-26, DHS-CISA TIC 3.0 Core Guidance Documents)	The organization has not prepared and planned to meet the goals of the TIC initiative, consistent with OMB M-19-26. Specifically, the agency has not defined and customized, as appropriate, its policies, procedures, and processes to implement TIC 3.0, including updating its network and system boundary policies, in accordance with OMB M-19-26. This includes, as appropriate, the TIC security capabilities catalog, TIC use cases, and TIC overlays. The agency has not defined processes to develop and maintain an accurate inventory of its network connections, including details on the service provider, cost, capacity, traffic volume, logical/physical configurations, and topological data for each connection.	The organization has prepared and planned to meet the goals of the TIC initiative, consistent with OMB M-19-26. Specifically, the agency has defined and customized, as appropriate, its policies, procedures, and processes to implement TIC 3.0, including updating its network and system boundary policies, in accordance with OMB M-19-26. This includes, as appropriate, incorporation of TIC security capabilities catalog, TIC use cases, and TIC overlays. The agency has defined processes to develop and maintain an accurate inventory of its network connections, including details on the service provider, cost, capacity, traffic volume, logical/physical configurations, and topological data for each connection.	The organization consistently implements TIC requirements based on OMB M-19-26. This includes consistent implementation of defined TIC security controls, as appropriate, and ensuring that that all agency traffic, including mobile and cloud, are routed through defined access points, as appropriate. The agency develops and maintains an accurate inventory of agency network connections, including details on the service provider, cost, capacity, traffic volume, logical/physical configurations, and topological data for each connection.	The organization, in accordance with OMB M-19-26, DHS guidance, and its cloud strategy is ensuring that its TIC implementation remains flexible and that its policies, procedures, and information security program are adapting to meet the security capabilities outlined in the TIC initiative, consistent with OMB M-19-26. The organization monitors and reviews the implemented TIC 3.0 use cases to determine effectiveness and incorporates new/different use cases, as appropriate.	

FY 2021 Inspector General FISMA Reporting Metrics v1.1
Protect Function Area (Configuration Management)

Question	Maturity Level				
	Ad Hoc	Defined	Consistently Implemented	Managed and Measurable	Optimized
23. To what extent has the organization defined and implemented configuration change control activities including: determination of the types of changes that are configuration controlled; review and approval/disapproval of proposed changes with explicit consideration of security impacts and security classification of the system; documentation of configuration change decisions; implementation of approved configuration changes; retaining records of implemented changes; auditing and review of configuration changes; and coordination and oversight of changes by the CCB, as appropriate (NIST SP 800-53 REV. 4: CM-2, CM-3 and CM-4; CSF: PR.IP-3).	The organization has not developed, documented, and disseminated its policies and procedures for managing configuration change control. Policies and procedures do not address, at a minimum, the necessary configuration change control related activities.	The organization has developed, documented, and disseminated its policies and procedures for managing configuration change control. The policies and procedures address, at a minimum, the necessary configuration change control related activities.	The organization consistently implements its change control policies, procedures, and processes, including explicit consideration of security impacts prior to change implementation. The organization utilizes lessons learned in implementation to make improvements to its change control policies and procedures	The organization monitors, analyzes, and reports qualitative and quantitative performance measures on the effectiveness of its change control activities and ensures that data supporting the metrics is obtained accurately, consistently, and in a reproducible format. In addition, the organization implements [organizationally defined security responses] if baseline configurations are changed in an unauthorized manner.	The organization utilizes automation to improve the accuracy, consistency, and availability of configuration change control and configuration baseline information. Automation is also used to provide data aggregation and correlation capabilities, alerting mechanisms, and dashboards on change control activities to support risk-based decision making across the organization.

FY 2021 Inspector General FISMA Reporting Metrics v1.1
Protect Function Area (Configuration Management)

Question	Maturity Level				
	Ad Hoc	**Defined**	**Consistently Implemented**	**Managed and Measurable**	**Optimized**
24. To what extent does the organization utilize a vulnerability disclosure policy (VDP) as part of its vulnerability management program for internet-accessible federal systems (OMB M-20-32 and DHS BOD 20-01)?	The organization has not developed, documented, and disseminated a comprehensive VDP.	The organization has developed, documented, and publicly disseminated a comprehensive VDP. The following elements are addressed: - The systems in scope - Types of testing allowed - Reporting mechanisms - Timely feedback - Remediation In addition, the organization has updated its vulnerability disclosure handling procedures to support the implementation of its VDP.	The organization consistently implements its VDP. In addition, the organization: - Has updated the relevant fields at the .gov registrar to ensure appropriate reporting by the public. -Ensures that newly launched internet accessible systems and services, and at least 50% of internet-accessible systems, are included in the scope of its VDP. -Increases the scope of systems covered by its VDP, in accordance with DHS BOD 20-01.	The organization monitors, analyzes, and reports on the qualitative and quantitative performance measures used to gauge the effectiveness of its vulnerability disclosure policy and disclosure handing procedures. In addition, all internet-accessible systems are included in the scope of the organization's VDP.	On a near real-time basis, the organization actively adapts its vulnerability disclosure policies and procedures and provides information to stakeholders and partners. Within the context of its enterprise risk management program, the organization considers the use of a Bug Bounty program. As appropriate, Bug Bounty programs are implemented in accordance with OMB M-20-32.
25. Provide any additional information on the effectiveness (positive or negative) of the organization's configuration management program that was not noted in the questions above. Taking into consideration the maturity level generated from the questions above and based on all testing performed, is the configuration management program effective?					

FY 2021 Inspector General FISMA Reporting Metrics v1.1
Protect Function Area (Identity and Access Management)

Table 8: Identity and Access Management

Question	Maturity Level				
	Ad Hoc	Defined	Consistently Implemented	Managed and Measurable	Optimized
26. To what extent have the roles and responsibilities of identity, credential, and access management (ICAM) stakeholders been defined, communicated, and implemented across the agency, and appropriately resourced (NIST SP 800-53 REV. 4: AC-1, IA-1, and PS-1; NIST SP 800-63-3 and 800-63A, B, and C; Federal Identity, Credential, and Access Management (FICAM) playbooks and guidance (see idmanagement.gov), OMB M-19-17)?	Roles and responsibilities at the organizational and information system levels for stakeholders involved in ICAM have not been fully defined and communicated across the organization.	Roles and responsibilities at the organizational and information system levels for stakeholders involved in ICAM have been fully defined and communicated across the organization. This includes, as appropriate, developing an ICAM governance structure to align and consolidate the agency's ICAM investments, monitor programs, and ensuring awareness and understanding.	Individuals are performing the roles and responsibilities that have been defined across the organization. The organization ensures that there is consistent coordination amongst organization leaders and mission owners to implement, manage, and maintain the organization's ICAM policy, strategy, process, and technology solution roadmap.	Resources (people, processes, and technology) are allocated in a risk-based manner for stakeholders to effectively implement identity, credential, and access management activities. Further, stakeholders are held accountable for carrying out their roles and responsibilities effectively.	In accordance with OMB M-19-17, the agency has implemented an integrated agency-wide ICAM office, team, or other governance structure in support of its ERM capability to effectively govern and enforce ICAM efforts.

FY 2021 Inspector General FISMA Reporting Metrics v1.1
Protect Function Area (Identity and Access Management)

Question	Maturity Level				
	Ad Hoc	Defined	Consistently Implemented	Managed and Measurable	Optimized
27. To what extent does the organization utilize a comprehensive ICAM policy, strategy, process, and technology solution roadmap to guide its ICAM processes and activities (FICAM, OMB M-19-17; NIST SP 800-53 REV. 4: AC-1 and IA-1; OMB M-19-17; SANS/CIS Top 20: 14.1; DHS ED 19-01; CSF: PR.AC-4 and 5)?	The organization has not developed a comprehensive ICAM policy, strategy, process, and technology solution road map to guide its ICAM processes and activities. In addition, the organization has not performed a review of current practices, identified gaps, and developed a transition plan to serve as an input to the ICAM policy, strategy, and technology solution road map.	The organization has developed a comprehensive ICAM policy, strategy, process, and technology solution road map to guide its ICAM processes and activities. The organization has developed milestones for how it plans to align with Federal initiatives, including strong authentication, the Federal ICAM architecture and OMB M-19-17, and phase 2 of DHS's Continuous Diagnostics and Mitigation (CDM) program, as appropriate.	The organization is consistently implementing its ICAM policy, strategy, process, and technology solution road map and is on track to meet milestones. The strategy encompasses the entire organization, aligns with the FICAM and CDM requirements, and incorporates applicable Federal policies, standards, playbooks, and guidelines. Further, the organization is consistently capturing and sharing lessons learned on the effectiveness of its ICAM policy, strategy, and road map and making updates as needed.	The organization integrates its ICAM strategy and activities with its enterprise architecture and the Federal ICAM architecture. The organization uses automated mechanisms (e.g. machine-based, or user-based enforcement), where appropriate, to manage the effective implementation of its ICAM policies, procedures, and strategy. Examples of automated mechanisms include network segmentation based on the label/classification of information stored; automatic removal/disabling of temporary/emergency/ inactive accounts; and use of automated tools to inventory and manage accounts and perform segregation of duties/least privilege reviews.	On a near real-time basis, the organization actively adapts its ICAM policy, strategy, and related processes and activities to a changing cybersecurity landscape to respond to evolving and sophisticated threats. The organization employs adaptive identification and authentication techniques to assess suspicious behavior and potential violations of its ICAM policies and procedures on a near-real time basis.

FY 2021 Inspector General FISMA Reporting Metrics v1.1
Protect Function Area (Identity and Access Management)

Question	Maturity Level				
	Ad Hoc	Defined	Consistently Implemented	Managed and Measurable	Optimized
28. To what extent has the organization developed and implemented processes for assigning position risk designations and performing appropriate personnel screening prior to granting access to its systems (NIST SP 800-53 REV. 4: PS-2 and PS-3; National Insider Threat Policy; CSF: PR.IP-11, OMB M-19-17)?	The organization has not defined its processes for assigning personnel risk designations and performing appropriate screening prior to granting access to its systems.	The organization has defined its processes for ensuring that all personnel are assigned risk designations and appropriately screened prior to being granted access to its systems. Processes have been defined for assigning risk designations for all positions, establishing screening criteria for individuals filling those positions, authorizing access following screening completion, and rescreening individuals on a periodic basis.	The organization ensures that all personnel are assigned risk designations, appropriately screened prior to being granted system access, and rescreened periodically.	The organization employs automation to centrally document, track, and share risk designations and screening information with necessary parties.	On a near-real time basis, the organization evaluates personnel security information from various sources, integrates this information with anomalous user behavior data (audit logging) and/or its insider threat activities, and adjusts permissions accordingly.
29. To what extent does the organization ensure that access agreements, including nondisclosure agreements, acceptable use agreements, and rules of behavior, as appropriate, for individuals (both privileged and non-privileged users) that access its systems are completed and maintained (NIST SP 800-53 REV. 4: AC-8, PL-4, and PS-6)?	The organization has not defined its processes for developing, documenting, and maintaining access agreements for individuals that access its systems.	The organization has defined its processes for developing, documenting, and maintaining access agreements for individuals that access its systems.	The organization ensures that access agreements for individuals are completed prior to access being granted to systems and are consistently maintained thereafter. The organization utilizes more specific/detailed agreements for privileged users or those with access to sensitive information, as appropriate.	The organization uses automation to manage and review user access agreements for privileged and non-privileged users. To the extent practical, this process is centralized.	On a near real-time basis, the organization ensures that access agreements for privileged and non-privileged users are maintained, as necessary.

FY 2021 Inspector General FISMA Reporting Metrics v1.1
Protect Function Area (Identity and Access Management)

Question	Maturity Level				
	Ad Hoc	Defined	Consistently Implemented	Managed and Measurable	Optimized
30. To what extent has the organization implemented strong authentication mechanisms (PIV or an Identity Assurance Level (IAL)3/Authenticator Assurance Level (AAL) 3 credential) for non-privileged users to access the organization's facilities [organization-defined entry/exit points], networks, and systems, including for remote access (HSPD-12; NIST SP 800-53 REV. 4: AC-17, IA-2, IA-5, IA-8, and PE-3; NIST SP 800-128; FIPS 201-2; NIST SP 800-63, 800-157; FY 2021 CIO FISMA Metrics: 2.4, 2.7, CSF: PR.AC-1 and 6; OMB M-19-17, and NIST SP 800-157)?	The organization has not planned for the use of strong authentication mechanisms for non-privileged users of the organization's facilities [organization-defined entry/exit points], systems, and networks, including for remote access. In addition, the organization has not performed digital identity risk assessments to determine which systems require strong authentication.	The organization has planned for the use of strong authentication mechanisms for non-privileged users of the organization's facilities [organization-defined entry/exit points], systems, and networks, including the completion of digital identity risk assessments.	The organization has consistently implemented strong authentication mechanisms for non-privileged users of the organization's facilities [organization-defined entry/exit points] and networks, including for remote access, in accordance with Federal targets. For instances where it would be impracticable to use the PIV card, the organization uses an alternative token (derived PIV credential) which can be implemented and deployed with mobile devices.	All non-privileged users utilize strong authentication mechanisms to authenticate to applicable organizational systems and facilities [organization-defined entry/exit points].	The organization has implemented an enterprise-wide single sign on solution and all of the organization's systems interface with the solution, resulting in an ability to manage user (non-privileged) accounts and privileges centrally and report on effectiveness on a near real-time basis.

FY 2021 Inspector General FISMA Reporting Metrics v1.1
Protect Function Area (Identity and Access Management)

Question	Maturity Level				
	Ad Hoc	Defined	Consistently Implemented	Managed and Measurable	Optimized
31. To what extent has the organization implemented strong authentication mechanisms (PIV or an Identity Assurance Level (IAL)3/Authenticator Assurance Level (AAL) 3 credential) for privileged users to access the organization's facilities [organization-defined entry/exit points], networks, and systems, including for remote access (HSPD-12; NIST SP 800-53 REV. 4: AC-17, PE-3; NIST SP 800-128; FIPS 201-2; NIST SP 800-63 and 800-157; OMB M-19-17, FY 2021 CIO FISMA Metrics: 2.3, 2.5, and 2.7; CSF: PR.AC-1 and 6; and DHS ED 19-01)?	The organization has not planned for the use of strong authentication mechanisms for privileged users of the organization's facilities [organization-defined entry/exit points], systems, and networks, including for remote access. In addition, the organization has not performed digital identity risk assessments to determine which systems require strong authentication.	The organization has planned for the use of strong authentication mechanisms for privileged users of the organization's facilities [organization-defined entry/exit points], systems, and networks, including the completion of digital identity risk assessments.	The organization has consistently implemented strong authentication mechanisms for privileged users of the organization's facilities [organization-defined entry/exit points], and networks, including for remote access, in accordance with Federal targets. For instances where it would be impracticable to use the PIV card, the organization uses an alternative token (derived PIV credential) which can be implemented and deployed with mobile devices.	All privileged users, including those who can make changes to DNS records, utilize strong authentication mechanisms to authenticate to applicable organizational systems.	The organization has implemented an enterprise-wide single sign on solution and all the organization's systems interface with the solution, resulting in an ability to manage user (privileged) accounts and privileges centrally and report on effectiveness on a near real-time basis.

FY 2021 Inspector General FISMA Reporting Metrics v1.1
Protect Function Area (Identity and Access Management)

Question	Maturity Level				
	Ad Hoc	Defined	Consistently Implemented	Managed and Measurable	Optimized
32. To what extent does the organization ensure that privileged accounts are provisioned, managed, and reviewed in accordance with the principles of least privilege and separation of duties? Specifically, this includes processes for periodic review and adjustment of privileged user accounts and permissions, inventorying and validating the scope and number of privileged accounts, and ensuring that privileged user account activities are logged and periodically reviewed (FY 2021 CIO FISMA Metrics: 2.3, 2.5, 2.6, and 2.7; OMB M-19-17, NIST SP 800-53 REV. 4: AC-1, AC-2, AC-5, AC-6, AC-17; AU-2, AU-3, AU-6, and IA-4; DHS ED 19-01; CSF: PR.AC-4).	The organization has not defined its processes for provisioning, managing, and reviewing privileged accounts.	The organization has defined its processes for provisioning, managing, and reviewing privileged accounts. Defined processes cover approval and tracking, inventorying and validating, and logging and reviewing privileged users' accounts.	The organization ensures that its processes for provisioning, managing, and reviewing privileged accounts are consistently implemented across the organization. The organization limits the functions that can be performed when using privileged accounts; limits the duration that privileged accounts can be logged in; limits the privileged functions that can be performed using remote access; and ensures that privileged user activities are logged and periodically reviewed.	The organization employs automated mechanisms (e.g. machine-based, or user-based enforcement) to support the management of privileged accounts, including for the automatic removal/disabling of temporary, emergency, and inactive accounts, as appropriate.	
33. To what extent does the organization ensure that appropriate configuration/connection requirements are maintained for remote access connections? This includes the use of appropriate cryptographic modules, system time-outs, and the monitoring and control of remote access sessions (NIST SP 800-53 REV. 4: AC-11, AC-12, AC-17, AC-19, AU-2, IA-7, SC-10, SC-13, and SI-4; CSF: PR.AC-3; and FY 2021 CIO FISMA Metrics: 2.10 and 2.11).	The organization has not defined the configuration/connection requirements for remote access connections, including use of FIPS 140-2 validated cryptographic modules, system time-outs, and monitoring and control of remote access sessions.	The organization has defined its configuration/connection requirements for remote access connections, including use of cryptographic modules, system time-outs, and how it monitors and controls remote access sessions.	The organization ensures that FIPS 140-2 validated cryptographic modules are implemented for its remote access connection method(s), remote access sessions time out after 30 minutes (or less), and that remote users' activities are logged and reviewed based on risk.	The organization ensures that end user devices have been appropriately configured prior to allowing remote access and restricts the ability of individuals to transfer data accessed remotely to non-authorized devices.	The organization has deployed a capability to rapidly disconnect remote access user sessions based on active monitoring. The speed of disablement varies based on the criticality of missions/business functions.

FY 2021 Inspector General FISMA Reporting Metrics v1.1
Protect Function Area (Identity and Access Management)

Question	Maturity Level				
	Ad Hoc	Defined	Consistently Implemented	Managed and Measurable	Optimized
34. Provide any additional information on the effectiveness (positive or negative) of the organization's identity and access management program that was not noted in the questions above. Taking into consideration the maturity level generated from the questions above and based on all testing performed, is the identity and access management program effective?					

FY 2021 Inspector General FISMA Metrics v1.1
Protect Function Area (Data Protection and Privacy)

Table 9: Data Protection and Privacy

Question	Maturity Level				
	Ad Hoc	Defined	Consistently Implemented	Managed and Measurable	Optimized
35. To what extent has the organization developed a privacy program for the protection of personally identifiable information (PII) that is collected, used, maintained, shared, and disposed of by information systems (NIST SP 800-122; NIST SP 800-37 (Rev. 2) Section 2.3, Task P-1 ; OMB M-20-04; OMB M-19-03; OMB A-130, Appendix I; CSF: ID.GV-3; NIST SP 800-53 REV. 4: AR-4 and Appendix J, FY 2020 SAOP FISMA metrics, Sections 1 through 4, 5(b), NIST Privacy Framework)?	The organization has not established a privacy program and related plans, policies, and procedures as appropriate for the protection of PII collected, used, maintained, shared, and disposed of by information systems. Additionally, roles and responsibilities for the effective implementation of the organization's privacy program have not been defined.	The organization has defined and communicated its privacy program plan and related policies and procedures for the protection of PII that is collected, used, maintained, shared, and/or disposed of by its information systems. In addition, roles and responsibilities for the effective implementation of the organization's privacy program have been defined and the organization has determined the resources and optimal governance structure needed to effectively implement its privacy program.	The organization consistently implements its privacy program by: - Dedicating appropriate resources to the program - Maintaining an inventory of the collection and use of PII - Conducting and maintaining privacy impact assessments and system of records notices for all applicable systems. - Reviewing and removing unnecessary PII collections on a regular basis (i.e., SSNs) - Using effective communications channels for disseminating privacy policies and procedures - Ensuring that individuals are consistently performing the privacy roles and responsibilities that have been defined across the organization	The organization monitors and analyses quantitative and qualitative performance measures on the effectiveness of its privacy activities and uses that information to make needed adjustments. The organization conducts an independent review of its privacy program and makes necessary improvements.	The privacy program is fully integrated with other security areas, such as ISCM, and other business processes, such as strategic planning and risk management. Further, the organization's privacy program is embedded into daily decision making across the organization and provides for continuous identification of privacy risks.

FY 2021 Inspector General FISMA Metrics v1.1
Protect Function Area (Data Protection and Privacy)

Question	Maturity Level				
	Ad Hoc	Defined	Consistently Implemented	Managed and Measurable	Optimized
36. To what extent has the organization implemented the following security controls to protect its PII and other agency sensitive data, as appropriate, throughout the data lifecycle. (NIST SP 800-53 REV. 4; Appendix J, SC-8, SC-28, MP-3, and MP-6; NIST SP 800-37 (Rev. 2); FY 2021 CIO FISMA Metrics: 2.8, 2.12; DHS BOD 18-02; CSF: PR.DS-1, PR.DS-2, PR.PT-2, and PR.IP-6)? • Encryption of data at rest • Encryption of data in transit • Limitation of transfer to removable media • Sanitization of digital media prior to disposal or reuse	The organization has not defined its policies and procedures in one or more of the specified areas.	The organization's policies and procedures have been defined and communicated for the specified areas. Further, the policies and procedures have been tailored to the organization's environment and include specific considerations based on data classification and sensitivity.	The organization's policies and procedures have been consistently implemented for the specified areas, including (i) use of FIPS-validated encryption of PII and other agency sensitive data, as appropriate, both at rest and in transit, (ii) prevention and detection of untrusted removable media, and (iii) destruction or reuse of media containing PII or other sensitive agency data.	The organization ensures that the security controls for protecting PII and other agency sensitive data, as appropriate, throughout the data lifecycle are subject to the monitoring processes defined within the organization's ISCM strategy.	The organization employs advanced capabilities to enhance protective controls, including (i) remote wiping, (ii) dual authorization for sanitization of media devices, (iii) exemption of media marking as long as the media remains within organizationally-defined control areas, and (iv) configuring systems to record the date the PII was collected, created, or updated and when the data is to be deleted or destroyed according to an approved data retention schedule.
37. To what extent has the organization implemented security controls to prevent data exfiltration and enhance network defenses? (NIST SP 800-53 REV. 4: SI-3, SI-7(8), SI-4(4) and (18), SC-7(10), and SC-18; FY 2021 CIO FISMA Metrics: 3.8; DHS BOD 18-01; DHS ED 19-01; CSF: PR.DS-5)?	The organization has not defined its policies and procedures related to data exfiltration, enhanced network defenses, email authentication processes, and mitigation against DNS infrastructure tampering.	The organization has defined and communicated it policies and procedures for data exfiltration, enhanced network defenses, email authentication processes, and mitigation against DNS infrastructure tampering.	The organization consistently monitors inbound and outbound network traffic, ensuring that all traffic passes through a web content filter that protects against phishing, malware, and blocks against known malicious sites. Additionally, the organization checks outbound communications traffic to detect encrypted exfiltration of information, anomalous traffic patterns, and elements of PII. Also, suspected malicious traffic is quarantined or blocked. In addition, the organization utilizes email authentication technology and ensures the use of valid encryption certificates for its domains.	The organization analyzes qualitative and quantitative measures on the performance of its data exfiltration and enhanced network defenses. The organization also conducts exfiltration exercises to measure the effectiveness of its data exfiltration and enhanced network defenses. Further, the organization monitors its DNS infrastructure for potential tampering, in accordance with its ISCM strategy. In addition, the organization audits its DNS records.	The organizations data exfiltration and enhanced network defenses are fully integrated into the ISCM and incident response programs to provide near real-time monitoring of the data that is entering and exiting the network, and other suspicious inbound and outbound communications.

FY 2021 Inspector General FISMA Metrics v1.1
Protect Function Area (Data Protection and Privacy)

Question	Maturity Level				
	Ad Hoc	Defined	Consistently Implemented	Managed and Measurable	Optimized
38. To what extent has the organization developed and implemented a Data Breach Response Plan, as appropriate, to respond to privacy events? (NIST SP 800-122; NIST SP 800-53 REV. 4: Appendix J, SE-2; FY 2020 SAOP FISMA metrics, Section 12; OMB M-17-12; and OMB M-17-25)?	The organization has not developed a Data Breach Response Plan that includes the agency's policies and procedures for reporting, investigating, and managing a privacy-related breach. Further, the organization has not established a breach response team that includes the appropriate agency officials.	The organization has defined and communicated its Data Breach Response Plan, including its processes and procedures for data breach notification. Further, a breach response team has been established that includes the appropriate agency officials.	The organization consistently implements its Data Breach Response plan. Additionally, the breach response team participates in table-top exercises and uses lessons learned to make improvements to the plan as appropriate. Further, the organization can identify the specific individuals affected by a breach, send notice to the affected individuals, and provide those individuals with credit monitoring and repair services, as necessary.	The organization monitors and analyzes qualitative and quantitative performance measures on the effectiveness of its Data Breach Response Plan, as appropriate. The organization ensures that data supporting metrics are obtained accurately, consistently, and in a reproducible format.	The organization's Data Breach Response plan is fully integrated with incident response, risk management, continuous monitoring, continuity of operations, and other mission/business areas, as appropriate. Further the organization employs automation to monitor for potential privacy incidents and takes immediate action to mitigate the incident and provide protection to the affected individuals.
39. To what extent does the organization ensure that privacy awareness training is provided to all individuals, including role-based privacy training (NIST SP 800-53 REV. 4: AR-5, FY 2020 SAOP FISMA Metrics, Sections 9 10, and 11)?	The organization has not defined its privacy awareness training program based on organizational requirements, its mission, and the types of PII that its users have access to. In addition, the organization has not developed role-based privacy training for individuals having responsibility for PII or activities involving PII.	The organization has defined and communicated its privacy awareness training program, including requirements for role-based privacy awareness training. Further, training has been tailored to the organization's mission and risk environment. (Note: Privacy awareness training topics should include, as appropriate: responsibilities under the Privacy Act of 1974 and E-Government Act of 2002, consequences for failing to carry out responsibilities, identifying privacy risks, mitigating privacy risks, and reporting privacy incidents, data collections and use requirements)	The organization ensures that all individuals receive basic privacy awareness training and individuals having responsibilities for PII or activities involving PII receive role-based privacy training at least annually. Additionally, the organization ensures that individuals certify acceptance of responsibilities for privacy requirements at least annually.	The organization measures the effectiveness of its privacy awareness training program by obtaining feedback on the content of the training and conducting targeted phishing exercises for those with responsibility for PII. Additionally, the organization make updates to its program based on statutory, regulatory, mission, program, business process, information system requirements, and/or results from monitoring and auditing.	The organization has institutionalized a process of continuous improvement incorporating advanced privacy training practices and technologies.

FY 2021 Inspector General FISMA Metrics v1.1
Protect Function Area (Data Protection and Privacy)

Question	Maturity Level				
	Ad Hoc	Defined	Consistently Implemented	Managed and Measurable	Optimized
40. Provide any additional information on the effectiveness (positive or negative) of the organization's data protection and privacy program that was not noted in the questions above. Taking into consideration the maturity level generated from the questions above and based on all testing performed, is the data protection and privacy program effective?					

FY 2021 Inspector General FISMA Metrics v1.1
Protect Function Area (Security Training)

Table 10: Security Training

Question	Maturity Level				
	Ad Hoc	Defined	Consistently Implemented	Managed and Measurable	Optimized
41. To what extent have the roles and responsibilities of security awareness and training program stakeholders been defined, communicated, and implemented across the agency, and appropriately resourced? (Note: this includes the roles and responsibilities for the effective establishment and maintenance of an organization wide security awareness and training program as well as the awareness and training related roles and responsibilities of system users and those with significant security responsibilities (NIST SP 800-53 REV. 4: AT-1; and NIST SP 800-50).	Roles and responsibilities have not been defined, communicated across the organization, and appropriately resourced.	Roles and responsibilities have been defined and communicated across the organization and resource requirements have been established.	Individuals are performing the roles and responsibilities that have been defined across the organization.	Resources (people, processes, and technology) are allocated in a risk-based manner for stakeholders to consistently implement security awareness and training responsibilities. Further, stakeholders are held accountable for carrying out their roles and responsibilities effectively.	
42. To what extent does the organization utilize an assessment of the skills, knowledge, and abilities of its workforce to provide tailored awareness and specialized security training within the functional areas of: identify, protect, detect, respond, and recover (NIST SP 800-53 REV. 4: AT-2 and AT-3; NIST SP 800-50: Section 3.2; Federal Cybersecurity Workforce Assessment Act of 2015; National Cybersecurity Workforce Framework v1.0; NIST SP 800-181; and CIS/SANS Top 20: 17.1)?	The organization has not defined its processes for assessing the knowledge, skills, and abilities of its workforce.	The organization has defined its processes for assessing the knowledge, skills, and abilities of its workforce to determine its awareness and specialized training needs and periodically updating its assessment to account for a changing risk environment.	The organization has assessed the knowledge, skills, and abilities of its workforce; tailored its awareness and specialized training; and has identified its skill gaps. Further, the organization periodically updates its assessment to account for a changing risk environment. In addition, the assessment serves as a key input to updating the organization's awareness and training strategy/plans.	The organization has addressed its identified knowledge, skills, and abilities gaps through training or talent acquisition.	The organization's personnel collectively possess a training level such that the organization can demonstrate that security incidents resulting from personnel actions or inactions are being reduced over time.

FY 2021 Inspector General FISMA Metrics v1.1
Protect Function Area (Security Training)

Question	Maturity Level				
	Ad Hoc	Defined	Consistently Implemented	Managed and Measurable	Optimized
43. To what extent does the organization utilize a security awareness and training strategy/plan that leverages its skills assessment and is adapted to its mission and risk environment? (Note: the strategy/plan should include the following components: the structure of the awareness and training program, priorities, funding, the goals of the program, target audiences, types of courses/material for each audience, use of technologies (such as email advisories, intranet updates/wiki pages/social media, web based training, phishing simulation tools), frequency of training, and deployment methods (NIST SP 800-53 REV. 4: AT-1; NIST SP 800-50: Section 3; CSF: PR.AT-1).	The organization has not defined its security awareness and training strategy/plan for developing, implementing, and maintaining a security awareness and training program that is tailored to its mission and risk environment.	The organization has defined its security awareness and training strategy/plan for developing, implementing, and maintaining a security awareness and training program that is tailored to its mission and risk environment.	The organization has consistently implemented its organization-wide security awareness and training strategy and plan.	The organization monitors and analyzes qualitative and quantitative performance measures on the effectiveness of its security awareness and training strategies and plans. The organization ensures that data supporting metrics are obtained accurately, consistently, and in a reproducible format.	The organization's security awareness and training activities are integrated across other security-related domains. For instance, common risks and control weaknesses, and other outputs of the agency's risk management and continuous monitoring activities inform any updates that need to be made to the security awareness and training program.

FY 2021 Inspector General FISMA Metrics v1.1
Protect Function Area (Security Training)

Question	Maturity Level				
	Ad Hoc	Defined	Consistently Implemented	Managed and Measurable	Optimized
44. To what extent does the organization ensure that security awareness training is provided to all system users and is tailored based on its mission, risk environment, and types of information systems? (Note: awareness training topics should include, as appropriate: consideration of organizational policies, roles and responsibilities, secure e-mail, browsing, and remote access practices, mobile device security, secure use of social media, phishing, malware, physical security, and security incident reporting (NIST SP 800-53 REV. 4: AT-1, AT-2; FY 2021 CIO FISMA Metrics: 2.15; NIST SP 800-50: 6.2; CSF: PR.AT-2; SANS Top 20: 17.4).	The organization has not defined its security awareness policies, procedures, and related material based on its mission, risk environment, and the types of information systems that its users have access to. In addition, the organization has not defined its processes for ensuring that all information system users are provided security awareness training [within organizationally defined timeframes] and periodically thereafter. Furthermore, the organization has not defined its processes for evaluating and obtaining feedback on its security awareness and training program and using that information to make continuous improvements.	The organization has defined and tailored its security awareness policies, procedures, and related material and delivery methods based on FISMA requirements, its, and the types of information systems that its users have access to. In addition, the organization has defined its processes for ensuring that all information system users including contractors are provided security awareness training [within organizationally defined timeframes] and periodically thereafter. Furthermore, the organization has defined its processes for evaluating and obtaining feedback on its security awareness and training program and using that information to make continuous improvements.	The organization ensures that its security awareness policies and procedures are consistently implemented. The organization ensures that all appropriate users complete the organization's security awareness training (or a comparable awareness training for contractors) [within organizationally defined timeframes] and periodically thereafter and maintains completion records. The organization obtains feedback on its security awareness and training program and uses that information to make improvements.	The organization measures the effectiveness of its awareness program by, for example, conducting phishing exercises and following up with additional awareness or training, and/or disciplinary action, as appropriate. The organization monitors and analyzes qualitative and quantitative performance measures on the effectiveness of its security awareness policies, procedures, and practices. The organization ensures that data supporting metrics are obtained accurately, consistently, and in a reproducible format.	The organization has institutionalized a process of continuous improvement incorporating advanced security awareness practices and technologies. On a near real-time basis (as determined by the agency given its threat environment), the organization actively adapts its security awareness policies, procedures, processes to a changing cybersecurity landscape and provides awareness and training, as appropriate, on evolving and sophisticated threats.

FY 2021 Inspector General FISMA Metrics v1.1
Protect Function Area (Security Training)

Question	Maturity Level				
	Ad Hoc	Defined	Consistently Implemented	Managed and Measurable	Optimized
45. To what extent does the organization ensure that specialized security training is provided to individuals with significant security responsibilities (as defined in the organization's security policies and procedures and in accordance with 5 Code of Federal Regulation 930.301) (NIST SP 800-53 REV. 4: AT-3 and AT-4; FY 2021 CIO FISMA Metrics: 2.15, and 5 Code of Federal Regulation 930.301)?	The organization has not defined its security training policies, procedures, and related materials based on its mission, risk environment, and the types of roles with significant security responsibilities. In addition, the organization has not defined its processes for ensuring that personnel with significant security roles and responsibilities are provided specialized security training [within organizationally defined timeframes] and periodically thereafter.	The organization has defined its security training policies, procedures, and related material based on FISMA requirements, its mission and risk environment, and the types of roles with significant security responsibilities. In addition, the organization has defined its processes for ensuring that personnel with assigned security roles and responsibilities are provided specialized security training [within organizationally defined time frames] and periodically thereafter.	The organization ensures that its security training policies and procedures are consistently implemented. The organization ensures that individuals with significant security responsibilities complete the organization's defined specialized security training (or comparable training for contractors) [within organizationally defined timeframes] and periodically thereafter. The organization also maintains completion records for specialized training taken by individuals with significant security responsibilities. The organization obtains feedback on its security training program and uses that information to make improvements.	The organization obtains feedback on its specialized security training content and processes and makes updates to its program, as appropriate. In addition, the organization measures the effectiveness of its specialized security training program by, for example, conducting targeted phishing exercises and following up with additional training, and/or disciplinary action, as appropriate. The organization monitors and analyzes qualitative and quantitative performance measures on the effectiveness of its security training policies, procedures, and practices. The organization ensures that data supporting metrics are obtained accurately, consistently, and in a reproducible format.	The organization has institutionalized a process of continuous improvement incorporating advanced security training practices and technologies. On a near real-time basis, the organization actively adapts its security training policies, procedures, processes to a changing cybersecurity landscape and provides awareness and training, as appropriate, on evolving and sophisticated threats.
46. Provide any additional information on the effectiveness (positive or negative) of the organization's security training program that was not noted in the questions above. Taking into consideration the maturity level generated from the questions above and based on all testing performed, is the security training program effective?					

DETECT FUNCTION AREA

Table 11: ISCM

Question	Maturity Level				
	Ad Hoc	**Defined**	**Consistently Implemented**	**Managed and Measurable**	**Optimized**
47. To what extent does the organization utilize information security continuous monitoring (ISCM) policies and an ISCM strategy that addresses ISCM requirements and activities at each organizational tier (NIST SP 800-37 (Rev. 2) Task P-7; NIST SP 800-137: Sections 3.1 and 3.6)?	The organization has not developed, tailored, and communicated its ISCM policies and an organization wide ISCM strategy.	The organization has developed, tailored, and communicated its ISCM policies and strategy. The following areas are included - Monitoring requirements at each organizational tier - The minimum monitoring frequencies for implemented controls across the organization. The criteria for determining minimum frequencies is established in coordination with organizational officials [e.g., senior accountable official for risk management, system owners, and common control providers] and in accordance with organizational risk tolerance. - The organization's ongoing control assessment approach - How ongoing assessments are to be conducted - Analyzing ISCM data, reporting findings, and reviewing and updating the ISCM policies, procedures, and strategy	The organization's ISCM policies and strategy are consistently implemented at the organization, business process, and information system levels. In addition, the strategy supports clear visibility into assets, awareness into vulnerabilities, up-to-date threat information, and mission/business impacts. The organization also consistently captures lessons learned to make improvements to the ISCM policies and strategy.	The organization monitors and analyzes qualitative and quantitative performance measures on the effectiveness of its ISCM policies and strategy and makes updates, as appropriate. The organization ensures that data supporting metrics are obtained accurately, consistently, and in a reproducible format. The organization has transitioned to ongoing control and system authorization through the implementation of its continuous monitoring policies and strategy.	The organization's ISCM policies and strategy are fully integrated with its enterprise and supply chain risk management, configuration management, incident response, and business continuity programs. The organization can demonstrate that it is using its ISCM policies and strategy to reduce the cost and increase the efficiency of security and privacy programs.

FY 2021 Inspector General FISMA Metrics v1.1
Detect Function Area (ISCM)

Question	Maturity Level				
	Ad Hoc	Defined	Consistently Implemented	Managed and Measurable	Optimized
48. To what extent have ISCM stakeholders and their roles, responsibilities, levels of authority, and dependencies been defined, communicated, and implemented across the organization (NIST SP 800-53 REV. 4: CA-1; NIST SP 800-137; CSF: DE.DP-1; NIST 800-37, Rev. 2 Task P-7 and S-5)	Roles and responsibilities have not been fully defined and communicated across the organization, including appropriate levels of authority and dependencies.	The organization has defined and communicated the structures of its ISCM team, roles and responsibilities of ISCM stakeholders, and levels of authority and dependencies.	Individuals are performing the roles and responsibilities that have been defined across the organization.	Resources (people, processes, and technology) are allocated in a risk-based manner for stakeholders to effectively implement ISCM activities. Further, stakeholders are held accountable for carrying out their roles and responsibilities effectively.	
49. How mature are the organization's processes for performing ongoing information system assessments, granting system authorizations, including developing and maintaining system security plans, and monitoring system security controls (OMB A-130, NIST SP 800-137: Section 2.2; NIST SP 800-53 REV. 4: CA-2, CA-6, and CA-7; NIST Supplemental Guidance on Ongoing Authorization; NIST SP 800-37 (Rev. 2) Task S-5; NIST SP 800-18, Rev. 1, NIST IR 8011; OMB M-14-03; OMB M-19-03)	The organization has not developed system level continuous monitoring strategies/policies that define its processes for performing ongoing security control assessments, granting system authorizations, including developing and maintaining system security plans, monitoring security controls for individual systems; and time based triggers for ongoing authorization.	The organization has developed system level continuous monitoring strategies/policies that define its processes for performing ongoing security control assessments, granting system authorizations, including developing and maintaining system security plans, and monitoring security controls for individual systems; and time based triggers for ongoing authorization. The system level strategy/policies address the monitoring of those controls that are not addressed by the organizational level strategy, as well as how changes to the system are monitored and reported.	The organization consistently implements its system level continuous monitoring strategies and related processes, including performing ongoing security control assessments, granting system authorizations, including developing and maintaining system security plans, and monitoring security controls to provide a view of the organizational security posture, as well as each system's contribution to said security posture. In conjunction with the overall ISCM strategy, all security control classes (management, operational, and technical) and types (common, hybrid, and system-specific) are assessed and monitored, and their status updated regularly (as defined in the agency's information security policy) in security plans.	The organization utilizes the results of security control assessments and monitoring to maintain ongoing authorizations of information systems, including the maintenance of system security plans.	The organization's system level ISCM policies and strategies are fully integrated with its enterprise and supply chain risk management, configuration management, incident response, and business continuity programs. The organization can demonstrate that it is using its system level ISCM policies and strategy to reduce the cost and increase the efficiency of security and privacy programs.

FY 2021 Inspector General FISMA Metrics v1.1
Detect Function Area (ISCM)

Question	Maturity Level				
	Ad Hoc	**Defined**	**Consistently Implemented**	**Managed and Measurable**	**Optimized**
50. How mature is the organization's process for collecting and analyzing ISCM performance measures and reporting findings (NIST SP 800-137)?	The organization has not identified and defined the qualitative and quantitative performance measures that will be used to assess the effectiveness of its ISCM program, achieve situational awareness, and control ongoing risk. Further, the organization has not defined how ISCM information will be shared with individuals with significant security responsibilities and used to make risk-based decisions.	The organization has identified and defined the performance measures and requirements that will be used to assess the effectiveness of its ISCM program, achieve situational awareness, and control ongoing risk. In addition, the organization has defined the format of reports, frequency of reports, and the tools used to provide information to individuals with significant security responsibilities.	The organization is consistently capturing qualitative and quantitative performance measures on the performance of its ISCM program in accordance with established requirements for data collection, storage, analysis, retrieval, and reporting.	The organization is able to integrate metrics on the effectiveness of its ISCM program to deliver persistent situational awareness across the organization, explain the environment from both a threat/vulnerability and risk/impact perspective, and cover mission areas of operations and security domains.	On a near real-time basis, the organization actively adapts its ISCM program to a changing cybersecurity landscape and responds to evolving and sophisticated threats in a timely manner.
51. Provide any additional information on the effectiveness (positive or negative) of the organization's ISCM program that was not noted in the questions above. Taking into consideration the maturity level generated from the questions above and based on all testing performed, is the ISCM program effective?					

RESPOND FUNCTION AREA

Table 12: Incident Response

Question	Maturity Level				
	Ad Hoc	Defined	Consistently Implemented	Managed and Measurable	Optimized
52. To what extent does the organization utilize an incident response plan to provide a formal, focused, and coordinated approach to responding to incidents (NIST SP 800-53 REV. 4: IR-8; NIST SP 800-61 Rev. 2, section 2.3.2; CSF, RS.RP-1, Presidential Policy Directive (PPD) 8 – National Preparedness)?	The organization has not developed an incident response plan to provide a roadmap for implementing its incident response capability.	The organization has developed a tailored incident response plan that addresses - Structure and organization of the incident response capability - High-level approach for how the incident response capability fits into the overall organization - Defines reportable incidents, including major incidents - Metrics for measuring the incident response capability - Resources and management support	The organization consistently implements its incident response plan. Further, the organization is consistently capturing and sharing lessons learned on the effectiveness of its incident response plan and making updates as necessary.	The organization monitors and analyzes the qualitative and quantitative performance measures that have been defined in its incident response plan to monitor and maintain the effectiveness of its overall incident response capability. The organization ensures that data supporting metrics are obtained accurately, consistently, and in a reproducible format.	The organization's incident response plan is fully integrated with risk management, continuous monitoring, continuity of operations, and other mission/business areas, as appropriate. In addition, the organization make near real-time updates to its incident response plan based on changing risk environments and threat information. The organization participates in DHS's Cyber Storm national level exercise, as appropriate, or other exercises, to assess, cybersecurity preparedness, and examine incident response processes.
53. To what extent have incident response team structures/models, stakeholders, and their roles, responsibilities, levels of authority, and dependencies been defined, communicated, and implemented across the organization (NIST SP 800-53 REV. 4: IR-7; NIST SP 800-83; NIST SP 800-61 Rev. 2; CSF, RS.CO-1, OMB M-20-04; FY 2021 CIO FISMA Metrics: Section 4; CSF: RS.CO-1; and US-CERT Federal Incident Notification Guidelines)?	Roles and responsibilities have not been fully defined and communicated across the organization, including appropriate levels of authority and dependencies.	The organization has defined and communicated the structures of its incident response teams, roles and responsibilities of incident response stakeholders, and associated levels of authority and dependencies. In addition, the organization has designated a principal security operations center or equivalent organization that is accountable to agency leadership, DHS, and OMB for all incident response activities.	Individuals are performing the roles and responsibilities that have been defined across the organization.	Resources (people, processes, and technology) are allocated in a risk-based manner for stakeholders to effectively implement incident response activities. Further, stakeholders are held accountable for carrying out their roles and responsibilities effectively.	

FY 2021 Inspector General FISMA Metrics v1.1
Respond Function Area (Incident Response)

Question	Maturity Level				
	Ad Hoc	Defined	Consistently Implemented	Managed and Measurable	Optimized
54. How mature are the organization's processes for incident detection and analysis? (NIST 800-53: IR-4 and IR-6; NIST SP 800-61 Rev. 2; OMB M-20-04; CSF: DE.AE-1, DE.AE-2 -5, PR.DS-6, RS.AN-1 and 4, and PR.DS-8; and US-CERT Incident Response Guidelines)	The organization has not defined and communicated its policies, procedures, and processes for incident detection and analysis. In addition, the organization has not defined a common threat vector taxonomy for classifying incidents and its processes for detecting, analyzing, and prioritizing incidents.	The organization has defined and communicated its policies, procedures, and processes for incident detection and analysis. In addition, the organization has defined a common threat vector taxonomy and developed handling procedures for specific types of incidents, as appropriate. In addition, the organization has defined its processes and supporting technologies for detecting and analyzing incidents, including the types of precursors and indicators and how they are generated and reviewed, and for prioritizing incidents.	The organization consistently implements its policies, procedures, and processes for incident detection and analysis. In addition, the organization consistently utilizes its threat vector taxonomy to classify incidents and consistently implements its processes for incident detection, analysis, and prioritization. In addition, the organization consistently implements, and analyzes precursors and indicators generated by, for example, the following technologies: intrusion detection/prevention, security information and event management (SIEM), antivirus and antispam software, and file integrity checking software. Further, the organization is consistently capturing and sharing lessons learned on the effectiveness of its incident detection policies and procedures and making updates as necessary.	The organization monitors and analyzes qualitative and quantitative performance measures on the effectiveness of its incident detection and analysis policies and procedures. The organization ensures that data supporting metrics are obtained accurately, consistently, and in a reproducible format. The organization utilizes profiling techniques to measure the characteristics of expected activities on its networks and systems so that it can more effectively detect security incidents. Examples of profiling include running file integrity checking software on hosts to derive checksums for critical files and monitoring network bandwidth usage to determine what the average and peak usage levels are on various days and times. Through profiling techniques, the organization maintains a comprehensive baseline of network operations and expected data flows for users and systems.	

FY 2021 Inspector General FISMA Metrics v1.1
Respond Function Area (Incident Response)

Question	Maturity Level				
	Ad Hoc	Defined	Consistently Implemented	Managed and Measurable	Optimized
55. How mature are the organization's processes for incident handling (NIST 800-53: IR-4; NIST SP 800-61, Rev. 2; CSF: RS.MI-1 and 2)	The organization has not defined its policies, procedures, and processes for incident handling to include containment strategies for various types of major incidents, eradication activities to eliminate components of an incident and mitigate any vulnerabilities that were exploited, and recovery of systems.	The organization has defined its policies, procedures, and processes for incident handling to include containment strategies for each key incident type. In developing its strategies, the organization takes into consideration: the potential damage to and theft of resources, the need for evidence preservation, service availability, time and resources needed to implement the strategy, effectiveness of the strategy, and duration of the solution. In addition, the organization has defined its processes to eradicate components of an incident, mitigate any vulnerabilities that were exploited, and recover system operations.	The organization consistently implements its incident handling policies, procedures, containment strategies, and incident eradication processes. In addition, the organization consistently implements processes to remediate vulnerabilities that may have been exploited on the target system(s), and recovers system operations. Further, the organization is consistently capturing and sharing lessons learned on the effectiveness of its incident handling policies and procedures and making updates as necessary.	The organization monitors and analyzes qualitative and quantitative performance measures on the effectiveness of its incident handling policies and procedures. The organization ensures that data supporting metrics are obtained accurately, consistently, and in a reproducible format. The organization manages and measures the impact of successful incidents and can quickly mitigate related vulnerabilities on other systems so that they are not subject to exploitation of the same vulnerability.	The organization utilizes dynamic reconfiguration (e.g., changes to router rules, access control lists, and filter rules for firewalls and gateways) to stop attacks, misdirect attackers, and to isolate components of systems.
56. To what extent does the organization ensure that incident response information is shared with individuals with significant security responsibilities and reported to external stakeholders in a timely manner (FISMA; OMB M-20-04; NIST SP 800-53 REV. 4: IR-6; US-CERT Incident Notification Guidelines; PPD-41; CSF: RS.CO-2 through 5; DHS Cyber Incident Reporting Unified Message)	The organization has not defined its policies, procedures, and processes to share incident response information with individuals with significant security responsibilities or its processes for reporting security incidents, including major incidents, to US-CERT and other stakeholders (e.g., Congress and the Inspector General, as applicable) in a timely manner.	The organization has defined its policies, procedures, and processes to report suspected security incidents to the organization's incident response capability within organization defined timeframes. In addition, the organization has defined its processes for reporting security incident information, including for major incidents, to US-CERT, law enforcement, the Congress and the Office of Inspector General, as appropriate.	The organization consistently shares information on incident activities with internal stakeholders. The organization ensures that security incidents are reported to US-CERT, law enforcement, the Office of Inspector General, and the Congress (for major incidents) in a timely manner. Further, the organization is consistently capturing and sharing lessons learned on the effectiveness of its incident reporting policies and procedures and making updates as necessary.	Incident response metrics are used to measure and manage the timely reporting of incident information to organizational officials and external stakeholders. The organization ensures that data supporting metrics are obtained accurately, consistently, and in a reproducible format.	The organization receives, retains, uses, and disseminates cyber threat indicators in accordance with the Cybersecurity Information Sharing Act of 2015.

FY 2021 Inspector General FISMA Metrics v1.1
Respond Function Area (Incident Response)

Question	Maturity Level				
	Ad Hoc	Defined	Consistently Implemented	Managed and Measurable	Optimized
57. To what extent does the organization collaborate with stakeholders to ensure on-site, technical assistance/surge capabilities can be leveraged for quickly responding to incidents, including through contracts/agreements, as appropriate, for incident response support (NIST SP 800-86; NIST SP 800-53 REV. 4: IR-4; OMB M-20-04; PPD-41).	The organization has not defined how it will collaborate with DHS and other parties, as appropriate, to provide on-site, technical assistance/surge resources/special capabilities for quickly responding to incidents. In addition, the organization has not defined how it plans to utilize DHS' Einstein program for intrusion detection/prevention capabilities for traffic entering and leaving the organization's networks.	The organization has defined how it will collaborate with DHS and other parties, as appropriate, to provide on-site, technical assistance/surge resources/special capabilities for quickly responding to incidents. This includes identification of incident response services that may need to be procured to support organizational processes. In addition, the organization has defined how it plans to utilize DHS' Einstein program for intrusion detection/prevention capabilities for traffic entering and leaving the organization's networks.	The organization consistently utilizes on-site, technical assistance/surge capabilities offered by DHS or ensures that such capabilities are in place and can be leveraged when needed. In addition, the organization has entered into contractual relationships in support of incident response processes (e.g., for forensic support), as needed. The organization has fully deployed DHS' Einstein 1 and 2 to screen all traffic entering and leaving its network through a TIC.	The organization utilizes Einstein 3 Accelerated, and/or other comparable tools or services, to detect and proactively block cyber-attacks or prevent potential compromises.	

FY 2021 Inspector General FISMA Metrics v1.1
Respond Function Area (Incident Response)

Question	Maturity Level				
	Ad Hoc	**Defined**	**Consistently Implemented**	**Managed and Measurable**	**Optimized**
58. To what extent does the organization utilize the following technology to support its incident response program? -Web application protections, such as web application firewalls -Event and incident management, such as intrusion detection and prevention tools, and incident tracking and reporting tools -Aggregation and analysis, such as security information and event management (SIEM) products -Malware detection, such as antivirus and antispam software technologies - Information management, such as data loss prevention - File integrity and endpoint and server security tools (NIST SP 800-137; NIST SP 800-61, Rev. 2; NIST SP 800-44)	The organization has not identified and defined its requirements for incident response technologies needed in one or more of the specified areas and relies on manual/procedural methods in instances where automation would be more effective.	The organization has identified and fully defined its requirements for the incident response technologies it plans to utilize in the specified areas. While tools are implemented to support some incident response activities, the tools are not interoperable to the extent practicable, do not cover all components of the organization's network, and/or have not been configured to collect and retain relevant and meaningful data consistent with the organization's incident response policy, plans, and procedures.	The organization has consistently implemented its defined incident response technologies in the specified areas. In addition, the technologies utilized are interoperable to the extent practicable, cover all components of the organization's network, and have been configured to collect and retain relevant and meaningful data consistent with the organization's incident response policy, procedures, and plans.	The organization evaluates the effectiveness of its incident response technologies and makes adjustments to configurations and toolsets, as appropriate.	The organization has institutionalized the implementation of advanced incident response technologies for analysis of trends and performance against benchmarks (e.g., simulation based technologies to continuously determine the impact of potential security incidents to its IT assets) and adjusts incident response processes and security measures accordingly.
59. Provide any additional information on the effectiveness (positive or negative) of the organization's incident response program that was not noted in the questions above. Taking into consideration the maturity level generated from the questions above and based on all testing performed, is the incident response program effective?					

RECOVER FUNCTION AREA

Table 13: Contingency Planning

Question	Maturity Level				
	Ad Hoc	Defined	Consistently Implemented	Managed and Measurable	Optimized
60. To what extent have roles and responsibilities of stakeholders involved in information systems contingency planning been defined, communicated, and implemented across the organization, including appropriate delegations of authority (NIST SP 800-53 REV. 4: CP-1, CP-2, and CP-3; NIST SP 800-34; NIST SP 800-84; FCD-1: Annex B)?	Roles and responsibilities have not been fully defined and communicated across the organization, including appropriate delegations of authority.	Roles and responsibilities of stakeholders have been fully defined and communicated across the organization, including appropriate delegations of authority. In addition, the organization has designated appropriate teams to implement its contingency planning strategies. Further, the organization has defined its policies and procedures for providing contingency training consistent with roles and responsibilities.	Individuals are performing the roles and responsibilities that have been defined across the organization. The organization ensures that contingency training is provided consistent with roles and responsibilities to ensure that the appropriate content and level of detail is included.	Resources (people, processes, and technology) are allocated in a risk-based manner for stakeholders to effectively implement system contingency planning activities. Further, stakeholders are held accountable for carrying out their roles and responsibilities effectively.	The organization incorporates simulated events into contingency training to facilitate effective response by stakeholders (internal and external) involved in information systems contingency planning and to measure the extent to which individuals are equipped to perform their roles and responsibilities.

FY 2021 Inspector General FISMA Metrics v1.1
Recover Function Area (Contingency Planning)

Question	Maturity Level				
	Ad Hoc	Defined	Consistently Implemented	Managed and Measurable	Optimized
61. To what extent does the organization ensure that the results of business impact analyses (BIA) are used to guide contingency planning efforts (NIST SP 800-53 REV. 4: CP-2; NIST SP 800-34, Rev. 1, 3.2; NIST IR 8286; FIPS 199; FCD-1; OMB M-19-03; FY 2021 CIO FISMA Metrics, Section 5; CSF:ID.RA-4)?	The organization has not defined its policies, procedures, and processes for conducting organizational and system-level BIAs and for incorporating the results into strategy and plan development efforts.	The organization has defined its policies, procedures, and processes for conducting organizational and system-level BIAs and for incorporating the results into strategy and plan development efforts.	The organization consistently incorporates the results of organizational and system level BIAs into strategy and plan development efforts. System level BIAs are integrated with the organizational level BIA and include: characterization of all system components, determination of missions/business processes and recovery criticality, identification of resource requirements, and identification of recovery priorities for system resources. The results of the BIA are consistently used to determine contingency planning requirements and priorities, including mission essential functions/high value assets.	The organization ensures that the results of organizational and system level BIA's are integrated with enterprise risk management processes, for consistently evaluating, recording, and monitoring the criticality and sensitivity of enterprise assets. As appropriate, the organization utilizes the results of its BIA in conjunction with its risk register to calculate potential losses and inform senior level decision making.	

FY 2021 Inspector General FISMA Metrics v1.1
Recover Function Area (Contingency Planning)

Question	Maturity Level				
	Ad Hoc	Defined	Consistently Implemented	Managed and Measurable	Optimized
62. To what extent does the organization ensure that information system contingency plans are developed, maintained, and integrated with other continuity plans (NIST SP 800-53 REV. 4: CP-2; NIST SP 800-34; FY 2021 CIO FISMA Metrics: 5.1; OMB M-19-03; CSF: PR.IP-9)?	The organization has not defined its policies, procedures, and processes for information system contingency plan (ISCP) development and maintenance. In addition, the organization has not developed templates to guide plan development; and system contingency plans are developed in an ad-hoc manner with limited integration with other continuity plans.	The organization has defined its policies, procedure, and processes for information system contingency plan development, maintenance, and integration with other continuity areas. The policies, procedures, and processes for ISCP include the following phases: activation and notification, recovery, and reconstitution.	Information system contingency plans are consistently developed and implemented for systems, as appropriate, and include organizational and system level considerations for the following phases: activation and notification, recovery, and reconstitution. In addition, system level contingency planning development/maintenance activities are integrated with other continuity areas including organization and business process continuity, disaster recovery planning, incident management, insider threat implementation plan (as appropriate), and occupant emergency plans.	The organization is able to integrate metrics on the effectiveness of its information system contingency plans with information on the effectiveness of related plans, such as organization and business process continuity, disaster recovery, incident management, insider threat implementation, and occupant emergency, as appropriate to deliver persistent situational awareness across the organization. The organization coordinates the development of ISCP's with the contingency plans of external service providers.	Information system contingency planning activities are fully integrated with the enterprise risk management program, strategic planning processes, capital allocation/budgeting, and other mission/business areas and embedded into daily decision making across the organization.
63. To what extent does the organization perform tests/exercises of its information system contingency planning processes (NIST SP 800-34; NIST SP 800-53 REV. 4: CP-3 and CP-4; FY 2021 CIO FISMA Metrics, Section 5; CSF: ID.SC-5 and CSF: PR.IP-10)?	The organization has not defined its policies, procedures, and processes for information system contingency plan testing/exercises. ISCP tests are performed in an ad-hoc, reactive manner.	Policies, procedures, and processes for information system contingency plan testing and exercises have been defined and include, as applicable, notification procedures, system recovery on an alternate platform from backup media, internal and external connectivity, system performance using alternate equipment, restoration of normal procedures, and coordination with other business areas/continuity plans, and tabletop and functional exercises.	Information system contingency plan testing and exercises are consistently implemented. ISCP testing and exercises are integrated, to the extent practicable, with testing of related plans, such as incident response plan/COOP/BCP.	The organization employs automated mechanisms to test system contingency plans more thoroughly and effectively. In addition, the organization coordinates plan testing with external stakeholders (e.g., ICT supply chain partners/providers), as appropriate.	Based on risk, the organization performs a full recovery and reconstitution of systems to a known state. In addition, the organization proactively employs [organization defined mechanisms] to disrupt or adversely affect the system or system component and test the effectiveness of contingency planning processes.

FY 2021 Inspector General FISMA Metrics v1.1
Recover Function Area (Contingency Planning)

Question	Maturity Level				
	Ad Hoc	Defined	Consistently Implemented	Managed and Measurable	Optimized
64. To what extent does the organization perform information system backup and storage, including use of alternate storage and processing sites, as appropriate (NIST SP 800-53 REV. 4: CP-6, CP-7, CP-8, and CP-9; NIST SP 800-34: 3.4.1, 3.4.2, 3.4.3; FCD-1; NIST CSF: PR.IP-4; FY 2021 CIO FISMA Metrics, Section 5; and NARA guidance on information systems security records)?	The organization has not defined its policies, procedures, processes, strategies, and technologies for information system backup and storage, including the use of alternate storage and processing sites and redundant array of independent disks (RAID), as appropriate. Information system backup and storage is performed in an ad- hoc, reactive manner.	The organization has defined its policies, procedures, processes, strategies, and technologies for information system backup and storage, including use of alternate storage and processing sites and RAID, as appropriate. The organization has considered alternative approaches when developing its backup and storage strategies, including cost, environment (e.g., cloud model deployed), maximum downtimes, recovery priorities, and integration with other contingency plans.	The organization consistently implements its policies, procedures, processes, strategies, and technologies for information system backup and storage, including the use of alternate storage and processing sites and RAID, as appropriate. Alternate processing and storage sites are chosen based upon risk assessments that ensure the potential disruption of the organization's ability to initiate and sustain operations is minimized. In addition, the organization ensures that these sites and are not subject to the same risks as the primary site. Furthermore, the organization ensures that alternate processing and storage facilities are configured with information security safeguards equivalent to those of the primary site, including applicable ICT supply chain controls. Furthermore, backups of information at the user- and system-levels are consistently performed, and the confidentiality, integrity, and availability of this information is maintained.	The organization ensures that its information system backup and storage processes, including use of alternate storage and processing sties, and related supply chain controls, are assessed, as appropriate, as part of its continuous monitoring program. As part of its continuous monitoring processes, the organization demonstrates that its system backup and storage and alternate storage and processing sites are configured to facilitate recovery operations in accordance with recovery time and recover point objectives.	

FY 2021 Inspector General FISMA Metrics v1.1
Recover Function Area (Contingency Planning)

Question	Maturity Level				
	Ad Hoc	Defined	Consistently Implemented	Managed and Measurable	Optimized
65. To what level does the organization ensure that information on the planning and performance of recovery activities is communicated to internal stakeholders and executive management teams and used to make risk based decisions (CSF: RC.CO-3; NIST SP 800-53 REV. 4: CP-2 and IR-4)?	The organization has not defined how the planning and performance of recovery activities are communicated to internal stakeholders and executive management teams and used to make risk-based decisions.	The organization has defined how the planning and performance of recovery activities are communicated to internal stakeholders and executive management teams.	Information on the planning and performance of recovery activities is consistently communicated to relevant stakeholders and executive management teams, who utilize the information to make risk-based decisions.	Metrics on the effectiveness of recovery activities are communicated to relevant stakeholders and the organization has ensured that the data supporting the metrics are obtained accurately, consistently, and in a reproducible format.	
66. Provide any additional information on the effectiveness (positive or negative) of the organization's contingency planning program that was not noted in the questions above. Taking into consideration the maturity level generated from the questions above and based on all testing performed, is the contingency program effective?					